



Security Feature Test for Ethernet switches

- Thesis work in Bachelor of Science in Networking Technology written at ABB Control Technologies

Henrik Grankvist and William Kvarnström

Supervisor: Stefan Löfgren
Thesis 15hp
Spring 2014
2014-10-08

ABB document number:
3BSE080303



Preface

This report is written at ABB Process Automation, business unit Control Technologies and is a thesis within Bachelor Program in Computer Network Engineering.

We want to thank the people who have been involved and helped us during our work at ABB and also helped with the report. These people are our supervisor at Mälardalen University and respondents at ABB. At the employer we want to especially thank our supervisor who offered this degree project for us.

Tomas Lindström, Cyber Security Manager, BU Control Technologies and supervisor

Stefan Willby, IIT Certification Engineer, Control Technologies

Esse Johansson, System Engineer, Control Technologies

Stefan Löfgren, Supervisor at Mälardalen University Västerås

Abstract

A new standard in network security for industrial control systems is about to be released by a number of working groups within the ISA99 organization. ABB has a certification program for network components that may be used together with the control system 800xA, which is named Industrial IT Certification. ABB now wants to introduce formal testing of network component's security features according to this standard.

The document IEC 62443-4-2 is the document within this standard that describes how the system requirements should be implemented on network components. This document is still a draft, so the document IEC 62443-3-3 which describes how the system requirements should be implemented on a whole industrial control system has been used to estimate the content of IEC 62443-4-2 when it is finished. Out of these two documents the requirements has been broken down into a test description which contains a number of tests to check which security features a switch has and that they work as described. Together with the test description, a test record template has been created to be used for documenting the result from the tests.

Finally a comparison was made where the results from a number of different network equipment could be compared against each other regarding their security features. This comparison will in the future make it easier for ABB's customers when they are in the process of buying new network equipment.

In short the more expensive brands of switches have in general more security features implemented, and desktop switches has more security features implemented than industrial switches, with certain exceptions. The buyer needs to ask himself if he really needs all the security features. The choice of what switch to buy all depends on the placement of the switch and what purpose it should fulfill.

Sammanfattning

En ny standard för nätverkssäkerhet för industriella styrsystem håller på att släppas av ett antal arbetsgrupper inom organisationen ISA99. ABB har ett certifieringsprogram för utrustning som får användas tillsammans med styrsystemet "System 800xA", som heter Industrial IT Certification. ABB vill nu införa formella tester av nätverksutrustningars säkerhetsegenskaper enligt denna standard.

Dokumentet IEC 62443-4-2 är det dokument inom standarden som beskriver hur systemkraven bör uppfyllas på nätverksutrustningar. Dock är detta dokument inte ännu färdigt, så dokumentet IEC 62443-3-3 som beskriver hur systemkraven bör uppfyllas i ett helt industriellt styrsystem har använts för att skapa en uppfattning om vad IEC 62443-4-2 kommer att innehålla när det är färdigt. Utifrån dessa två dokument bröts kraven ner till en testbeskrivning som är utformat med ett flertal tester för att kontrollera vilka säkerhetsfunktioner en switch har och att de fungerar. Tillsammans med testbeskrivningen har ett testprotokoll skapats som används till att anteckna resultat från testerna.

Slutligen kunde en jämförelse framställas där resultatet av ett flertal olika testade enheter jämförs mot varandra gällandes deras säkerhetsfunktioner. Denna jämförelse ska i framtiden underlätta för ABBs kunder vid val av ny nätverksutrustning.

Sammanfattningsvis kan man se att de dyrare switcharna generellt har mer säkerhetsfunktioner, med vissa undantag. Det man som inköpare bör fråga sig är om man behöver alla säkerhetsfunktioner. Valet av switch beror helt på placering och vilket ändamål den ska uppfylla.

Abbreviations

3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
BPDU	Bridge Protocol Data Unit
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IANA	Internet Assigned Number Authority
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
EAP	Extensible Authentication Protocol
EAPOL	Extensible Authentication Protocol over LAN
IP	Internet Protocol
MAC	Media Access Control
MD5	Message Digest 5
NTP	Network Time Protocol
OSI	Open System Interconnection
RADIUS	Remote Authentication Dial-in User Services
RSTP	Rapid Spanning Tree Protocol
DoS	Denial of Service
SHA1	Secure Hash Algorithm 1
SNTP	Simple Network Time Protocol
MITM	Man-in-the-middle
SSH	Secure Shell
SSL	Secure Socket Layer
TACACAS+	Terminal Access Controller Access Control System Plus
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network

Who has written what

Henrik

- 1.1 Background
- 1.2 Purpose
- 2.1 Theoretical framework
- 2.2 Thesis
- 2.3 Method critics
- 3.1 User management
 - 3.1.1 Local user database
 - 3.1.2 Centralized authentication
 - 3.1.2.1 RADIUS
 - 3.1.2.2 TACACS+
 - 3.2 Connection methods
 - 3.2.1 Local connection
 - 3.2.2 Remote connection
 - 3.2.3.1 Telnet
 - 3.2.3.2 HTTP
 - 3.2.3.3 SNMP (v1/v2c)
 - 3.2.4.1 SSH
 - 3.2.4.2 HTTPS
 - 3.2.4.3 SNMPv3
 - 3.2.5 Limit connections
- 4 Thesis
 - 4.1 ISA99
 - 4.2 IEC 62443
 - 4.2.1 IEC 62443-3-3
 - 4.2.2 IEC 62443-4-2
 - 4.4 Test description
 - 4.4.1 Scope of use
 - 4.4.3 Traceability
 - 4.4.4.4 Limit connections
 - 4.4.4.5 Secure connection methods
 - 4.4.4.6 SNMP
 - 4.4.4.7 Audit logging
 - 4.4.4.8 Login
 - 4.4.4.9 Time
 - 4.4.4.10 DHCP
 - 4.4.4.12 Network segmentation
 - 4.4.4.13 Backup of configuration file
 - 4.4.4.14 Spanning Tree
 - 4.6 Comparison chart
- 5.0 Conclusions

William

- 1.3 Limitations
 - 3.1.3 Passwords
 - 3.3.1 802.1x
 - 3.3.2 DHCP
 - 3.3.2.1 DHCP-Snooping
 - 3.3.2.2 DHCP rate-limit
 - 3.3.3 Port restrictions
 - 3.4 Spanning Tree
 - 3.4.1 BPDU Guard
 - 3.4.2 Root Guard
 - 3.5 Time synchronization
 - 3.5.1 NTP
 - 3.5.2 SNTP
 - 3.5.3 Authentication
 - 3.6 Audit logs
 - 3.6.1 Syslog
 - 3.7 Confidentiality
 - 3.8 Server
 - 3.8.1 Ubuntu
 - 3.8.2 Virtualization
 - 3.9 Attacks
 - 3.9.1 Denial of Service
 - 3.9.2 Eavesdropping
 - 3.9.3 Reconnaissance
 - 4.3 Lab room
 - 4.3.1 Equipment
 - 4.4.2 Structure
 - 4.4.2.1 The purpose of the test
 - 4.4.2.2 Preparation and data input
 - 4.4.2.3 Procedure
 - 4.4.2.4 Expected result
 - 4.4.4.1 Local account management
 - 4.4.4.2 Centralized account management
 - 4.4.4.3 Local and remote connections
 - 4.4.4.11 Port security against users
 - 4.4.4.15 Confidentiality
 - 4.5 Test record
- 5.0 Conclusions
- 5.1 Future work

Table of Contents

1	Introduction	10
1.1	Background	10
1.2	Purpose	10
1.3	Limitation	11
2	Method	12
2.1	Theoretical framework	12
2.2	Thesis	12
2.3	Method critics	12
3	Theoretical framework	14
3.1	User management.....	14
3.1.1	Local user database.....	14
3.1.2	Centralized authentication.....	14
3.1.3	Passwords	15
3.2	Connection methods.....	16
3.2.1	Local connection	16
3.2.2	Remote connection.....	16
3.2.3	Unsecure remote connection methods	17
3.2.4	Secure remote connection methods	17
3.2.5	Limit connections	18
3.3	Port security against users	18
3.3.1	802.1x.....	18
3.3.2	DHCP	19
3.3.3	Port restrictions	20
3.4	Spanning Tree	20
3.4.1	BPDU Guard	21
3.4.2	Root Guard.....	22
3.5	Time synchronization.....	22
3.5.1	NTP	22
3.5.2	SNTP	22
3.5.3	Authentication	22
3.6	Audit logs	23
3.6.1	Syslog	23
3.7	Confidentiality.....	23
3.8	Server	23

3.8.1	Ubuntu	23
3.8.2	Virtualization	24
3.9	Attacks.....	25
3.9.1	Denial of Service.....	25
3.9.2	Eavesdropping.....	25
3.9.3	Man in the Middle.....	25
3.9.4	Reconnaissance.....	26
4	Thesis	27
4.1	ISA99	27
4.2	IEC 62443	28
4.2.1	IEC 62443-3-3	28
4.2.2	IEC 62443-4-2	28
4.3	Lab room	29
4.3.1	Equipment.....	30
4.4	Test description.....	31
4.4.1	Scope of use	31
4.4.2	Structure	31
4.4.3	Traceability.....	32
4.4.4	Tests	32
4.5	Test record	36
4.6	Comparison chart.....	36
5	Conclusion.....	37
5.1	Future work.....	37
6	References	39
6.1	IEC 62443	39
6.2	Books.....	39
6.3	Internet references	39
6.3.1	Cisco documentation	39
6.3.2	RFC	40
6.3.3	Other internet references.....	40
7	Appendices.....	43
7.1	Mail interview	43
7.2	Comparison chart.....	45

Table of Figures

Figure 1 RADIUS / TACACS+	14
Figure 2 Public and private key	17
Figure 3 802.1x.....	19
Figure 4 Spanning Tree ports	21
Figure 5 Ubuntu	24
Figure 6 Man in the middle attack.....	25
Figure 7 IEC 62443, [ISA62443]	27
Figure 8 Lab topology.....	29

1 Introduction

1.1 Background

Network security in an industrial network is probably more important than in any other network. Industrial networks include important social functions such as power plants that generate electrical power for an entire city. Therefore it is extremely important to mitigate and protect against attacks on industrial networks. Interruption or disturbance in industrial networks can cause high severity damages on the social community and in worst cases cost peoples life.

A network is not more secure than its weakest link and therefore every part of a network needs to be secured. A power plant or oil platform is dependent on its network for it to function. If an attack was successfully conducted on such a network it could cause a tremendous damage and loss of income.

A new standard for network security for industrial control systems named IEC 62443 is about to be released by a number of working groups within the ISA99 organization, which is part of the International Society of Automation (ISA). ISA's purpose is to establish standards, recommended practices, technical reports, and related information regarding safety aspects to be used for implementation and production of control systems. IEC 62443-3-3 describes the security requirements on a whole industrial control system while IEC 62443-4-2 describes how these requirements should be fulfilled in host devices, applications, embedded systems and network devices.

ABB has a certification program for equipment that can be used in together with system 800xA, called Industrial IT Certification. System 800xA is a fully redundant control system used by industries, mines, and oil platforms etc, to control and supervise the process. ABB now wants to include formal testing of network device's security features according to IEC 62443-3-3 and IEC 62443-4-2. For this a test description and a test record is needed. A comparison will also be created to show the result from the tests in an easy comprehensible way.

IEC 62443-4-2 is still a draft, which forces one to read IEC 62443-3-3 to make an estimation on what IEC 62443-4-2 will contain when it is finished. These documents contain parts that are not applicable on switches. A choice whether or not a requirement should be included as a test in the test description then had to be made.

Control system users start to realize that security have to be implemented in to the network, but it is hard to know which switches are secure. There are at the moment to available comparison between switches. There are switches in all possible price ranges, but do you really get the securest switch by buying the most expensive one?

1.2 Purpose

The purpose of this thesis work is to create an easily comprehensible test description on how to verify that a switch within industrial data communication fulfills the requirements that are set in IEC 62443-4-2, and to verify the test descriptions usefulness by conducting the tests on a number of switches.

Together with the test description, a test record needs to be created, where the results from the testing are recorded. In this test record a detailed guide on how the test's requirements were met will be explained by writing the commands that were written or what menus that were pressed.

The result from the test description is what makes the foundation of the comparison that will be made between the different switches that were tested. The comparison should be easy to understand and make it obvious to what switch is more secure than the other. This comparison will be available to ABB's customers to ease the choice of switches when buying new equipment.

1.3 Limitation

Initially it was said that a configuration description would be included in the work. This would be a document containing the exact steps in detail for each tested device of what is done and how it is done during the tests. This was later changed during an early meeting where the supervisor at ABB chose to reject this idea and instead include a detailed description on only a few tested devices. This was voluntarily chosen to be done on all devices that have been tested with an exact description for each step what has to be done, whether it be the CLI or GUI. These descriptions can be helpful for future jobs when performing tests on similar devices.

The tests have only relied on the security features in the switch's software. No tests on the switch's hardware have been implemented. Nor how well it manages a penetration test, which is an attack with the intention to find any security weaknesses and potentially gaining access to the device or other types of attacks such as manipulation of the package has been implemented.

2 Method

2.1 Theoretical framework

The theory part of this report discusses the theoretical knowledge needed to understand the tests that have been created in the test description. The theory part's references have primarily been original sources, books and the manufacturers own data sheets. Original sources means the original documents for the different protocols that are used in a switch. These protocols were standardized in RFCs' or by IETF and are available on the internet. The times where internet articles needed to be used as references the technical information has been verified by checking other pages for the same information.

2.2 Thesis

This thesis work is based on the new standard that the ISA99 organization is about to release: IEC 62443. The first step was to study the document IEC 62443-4-2, but because that document is not yet finished, the IEC 62443-3-3 document also had to be studied, so that the content that is not finished in IEC 62443-4-2 could be estimated. The documents are related to each other and covers the information on different depths. All the requirements in IEC 62443-4-2 are not applicable on switches and is something that has to be handled with care.

The creation of the tests that are included in the test description has largely been done based on previous knowledge. The knowledge has been obtained from the certificates and courses that has been studied within the area during our education. In some cases literature has been used and then the original sources has been attempted to be used as widely as possible. Some tests have been experimented when the design of the test has not been obvious. A switch's functionality must be verified through a test to be valid. A function that has not been possible to be verified through a test has not been approved.

Books covered in courses during our education that have been indirectly used to create the tests are "Implementing Cisco IP Switches Networks (SWITCH)" [SWITCH] and "CCNP Security SECURE" [CCNP-Security-Secure].

The test description's layout and content must be comprehensible, even for people that not necessarily possess the same knowledge as one that has read courses at the university or possesses certifications within the area. That is why detailed instructions are needed for every test. These instructions have been verified by the person at ABB that will later conduct these tests by performing them using the test description and later comment on the content so that it could be improved.

The comparison that will show how secure a switch is has been created in Microsoft Excel where diagrams can be automatically created. After a first draft of the comparison, the ABB employees that were involved in the thesis came with their thoughts on the design and coloring so that the comparison could be further improved.

2.3 Method critics

The information in the theoretical part has largely been referring to credible sources, such as original sources, books and data sheets. However, some of the information has been taken from less credible

internet sources. This information can be both biased and be hard to verify, that is why several articles dealing with the same subject have been used to personally create an impression.

3 Theoretical framework

This part of the report deals with the theoretical knowledge needed to understand the background of the tests included in the test description which is explained later in the thesis part of this report.

3.1 User management

AAA which is the acronym for Authentication, Authorization and Accounting is the term often used instead of user management. User management is an important part in network security because it controls who can login to a network device. The management can either be handled locally on the device itself or on a centralized server which controls the user management for all network devices in the network.

It is considered more secure to use a centralized authentication method because all the password are handled at one location, instead of locally on every single device.

3.1.1 Local user database

To be able to login to a network device you need a username and a password. These are saved in the local database of the network device, if a centralized authentication method is currently not in use. The disadvantage with using the local database is that it is a lot of work to change a password on a user account if the same password is used on all network devices, or if different accounts are used on all the network devices, it makes it hard to remember which account is located on what switch.

The local user database is however useful as a backup method if the centralized authentication server has failed. It is then very practical to have a local user on the network device with an advanced password that would not otherwise be used so that maintenance work still can be performed.

3.1.2 Centralized authentication

A more scalable solution than using a local user database is to assign the authentication of user accounts to a server. The advantage of a centralized method is that user accounts only have to be added on the server, instead of added on every single network device that this account needs to be able to be used on. This also has a positive effect on security because user accounts and password can easily be changed if a user account's login credentials would have been compromised. [TACACS+vsRADIUS]

There are two common protocols that are used for the communication between the network device and the server. The two protocols that are discussed in this report are RADIUS and TACACS+, where RADIUS is a IETF-standard and TACACS+ is a proprietary protocol developed by the company Cisco, but is also available on a few other manufacturers devices as well.

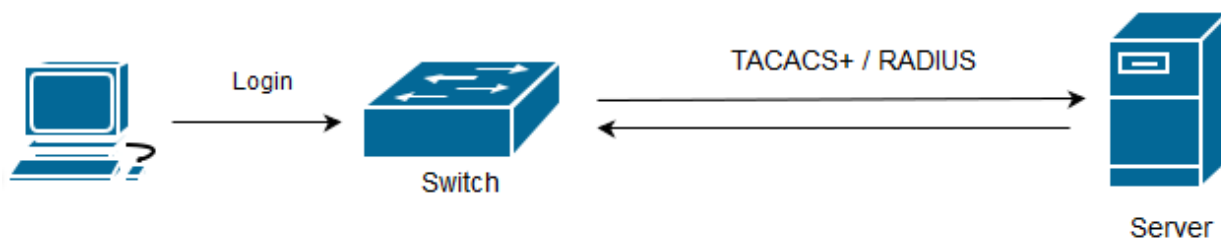


Figure 1 RADIUS / TACACS+

3.1.2.1 RADIUS

RADIUS is an IETF-standard and handles authentication of user accounts and accounting of changes being done. RADIUS uses UDP and has been assigned port 1812 for authentication and 1813 for accounting, by IANA [RFC2865], which is an organization that is responsible for the distribution of IP addresses and the development of Internet's structure. [IANA]

There are two disadvantages of RADIUS compared to TACACS+ and these are that RADIUS uses UDP and will because of the design of this protocol not resend packets, even though they are lost along the way or destroyed in some way. This is because UDP is not using any sequence numbers or ACK-packets that keep track of what packets have been sent and received successfully [DATAKOM]. RADIUS has added additional variables for retransmits and timeouts to compensate for this, but it does not compare to the functionality of TCP. [TACACS+vsRADIUS]

The second disadvantage is that the traffic between the network device and the server is not encrypted, only the password is encrypted, while the user account is sent in cleartext. This could lead to an intrusion attack where the attacker is guessing the password using some kind of program. [TACACS+vsRADIUS]

The advantage with RADIUS is that it is a standard and is therefore supported by all network devices that supports centralized authentication. This also leads to that there are more ways to authenticate users using RADIUS. An easy solution is to install a program where you are using a separate user database, while a more scalable solution for a large company would be to migrate the authentication of users into Active Directory on a Windows server for example.

3.1.2.2 TACACS+

TACACS+ is just like RADIUS a protocol used for the communication between the network device and the server when a user tries to authenticate. TACACS+ is better suited for larger networks than RADIUS is. This is because TACACS+ uses TCP and has therefore all the benefits that comes with it, such as retransmissions of lost packets, which is easily done if a network device along the path is congested by traffic at that particular moment. [TACACS+vsRADIUS]

A useful feature in TACACS+ is that it splits the authentication and authorization of users [TACACS+vsRADIUS]. This makes it possible to allow a user to login on a switch but only allow it to perform certain commands. This feature also applies better for larger companies because they are more likely to have different levels on their employees who have different permissions to make certain changes.

One of the bigger advantages of TACACS+ is that all of its communication between the network component and the server is encrypted, which mitigates that any unauthorized person can find out the username by listening to the network traffic. [TACACS+vsRADIUS]

3.1.3 Passwords

Bad handling of passwords is something that can cause intrusion. Employees are forced to use too complex passwords because of the company's password policy that forces them to write down their passwords on post-it notes that are left on their desktop. This is a big security risk and makes it possible

for anyone to login in to that persons user account. It is important to find a good balance between complexity and security. [ArsTechnica]

A password policy can contain the following requirements:

- A minimum number of characters
- A minimum number of lowercase letters
- A minimum number of uppercase letters
- A minimum number of non-numerical characters
- A maximum lifetime
- A minimum lifetime
- The password cannot be reused for a number of times

[MicrosoftPasswordPolicy]

3.2 Connection methods

To connect to a network device there are two available methods; locally and remotely. A local connection is normally through a console port on the network device which is directly connected from the user's computer to the network device. This normally gives the user a text based interface, or as it is more commonly called command line interface (CLI), which can be used to write commands in a text format. The other method is by using some kind of remote connection. This method can supply both a text based and a graphical interface and can be either secure or unsecure.

3.2.1 Local connection

A local connection to a network device is done by connecting a cable to the network device's console port to the computer which it will be configured from, it is therefore nothing in between which can listen to the information being sent. The configuration of the network device is done through a terminal emulator and is therefore text based.

Because the computer is directly connected to the device without an intermediate network; no encryption is needed. Network devices should also be out of reach for unauthorized persons because there is often special privileges for the one connected to the console port. These special privileges could be to perform a password recovery. [HARDEN]

3.2.2 Remote connection

A remote session can either be text based (CLI) or have a graphical interface (GUI). The two most common protocols for a text based remote connection are Telnet and SSH. For a graphical remote connection either HTTP or HTTPS are usually used. Telnet and HTTP both send all their information in cleartext over the network, while SSH and HTTPS use encryption.

3.2.3 Unsecure remote connection methods

3.2.3.1 Telnet

Telnet is an old protocol that is described in RFC 854. The protocol is used to connect to devices through the CLI [RFC854]. Telnet has no security implemented, so all its information is sent in cleartext. This makes both the username and the password easy to read for a program intended for listening to traffic on the network. Because of this, Telnet should always be avoided if possible. [COMP-GUIDE]

3.2.3.2 HTTP

HTTP is used by web browsers to retrieve web pages from servers. The web browser can connect to the network device's GUI. This gives a more user friendly interface which can be used to configure a network device. HTTP is just like Telnet completely unsecure and all its information is sent in cleartext. Because of this, HTTP should also be avoided if possible. [RFC2616]

3.2.3.3 SNMP (v1/v2c)

SNMP is a common and powerful administration tool. SNMP can retrieve information, but also configure a device [NET-SNMP]. SNMP sends all its information unencrypted and often uses the default-community-strings "public" to read information, and "private" to write information. SNMP version 1 and version 2c are protocols that should not be activated unnecessarily because unauthorized persons can get hold of a lot of information about the network with the use of SNMP. If the write community-string is known, a lot of damage can be done to the network.

SNMP is used mainly by monitoring programs by collecting information from all the network devices in the network and monitors the amount of CPU and memory is being used and then showing the results in graphs. [NET-SNMP]

3.2.4 Secure remote connection methods

3.2.4.1 SSH

SSH is a protocol that is used just like Telnet to connect to a device's CLI. The difference is that SSH uses encryption and therefore makes it impossible for unauthorized persons to read the information sent between the devices. [RFC4253]

SSH uses asymmetric encryption, which means that the two communicating creates a public and a private key, each. The public key is known by everyone. The first device's public key is used by the second device to encrypt the message that will be sent to the first device. The trick is that the message can only be decrypted by using the first device's private key, which only the first device possesses. [RFC4253]

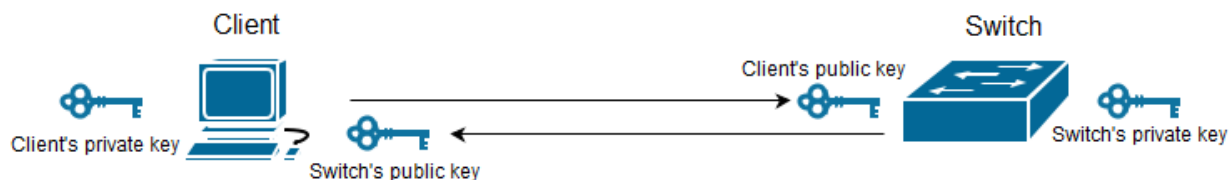


Figure 2 Public and private key

3.2.4.2 HTTPS

HTTPS is HTTP on top of the SSL/TLS protocol which uses X.509 certificates and therefore also uses asymmetric encryption. For the HTTPS server to be trusted, the certificate must be issued by a trusted Certificate Authority (CA). [HTTPS]

3.2.4.3 SNMPv3

SNMP version 3 adds authentication and encryption to the original versions of the SNMP protocol. Instead of using only one community-string, as in the previous versions, SNMPv3 uses a username, an authentication password and an encryption key to authenticate to a network device [CCNP-Security-Secure]. On some devices, however, the authentication password and encryption key is the same password.

Authentication can either be done with the protocols MD5 or SHA1 [RFC2574] and encryption can be done with either DES [RFC2574], 3DES or AES [SNMP].

SNMPv3 has three different modes; NoAuthNoPriv, AuthNoPriv and AuthPriv. NoAuthNoPriv is communication without authentication and encryption. This mode is backwards compatible with earlier versions of SNMP, where the username in SNMPv3 is used as the community-string. AuthNoPriv uses authentication, but without encryption, while AuthPriv uses both authentication and encryption and is therefore the safest option. [RFC2571]

3.2.5 Limit connections

To enhance the security on network devices further, a limit can be set from where a connection can come from. Administrators often sit on their own IP subnet and the rule can be configured to only allow administration of devices from that particular subnet. This action with the combination of a secure remote connection method makes it hard for any unauthorized persons to take control of a device.

Connections can also be limited in number. It is not often that there is more than one administrator logged in at the same time configuring a device, therefore it should not be an infinite number of connections possible. A connection to a device allocates resources from the device, even if the person connecting does not have the correct login credentials. This could lead to a potential DoS attack if the network device becomes too burdened with all the open connections to the device.

3.3 Port security against users

3.3.1 802.1x

802.1x is an IEEE standard for port-based access to network resources by users and machines. It is a technology that increases the security requirements for a client to connect to a local network. A client that connects to the network must enter additional information in terms of a username and a password to authenticate themselves and be granted access to the network. This is something that is used mainly in wireless networks.

Port-based authentication consists of three parts, a supplicant, an authenticator and an authentication server. The supplicant is the computer or user that wants to connect to the network and is prompted for credentials when it connects its network cable or logs in on their computer. Authenticator is usually an access point or a switch that is configured to authenticate clients attempting to connect. Login details given by the client is sent to the authenticator which further sends it to the authentication server, which

verifies that the information is correct. If the information is correct the server notifies the authenticator which then grants access to the local network for the supplicant. The port remains in a closed state until the user credentials have been verified and accepted by the server. On the authentication server the users are centrally stored on any kind of application with support for 802.1x authentication, such as RADIUS. [Cisco8021x]

If a client disconnect and reconnect the network cable it is required to enter credentials again to authenticate to the network. This means that no outsider can authenticate themselves using someone else's network cable, without the need for additional login credentials to connect to the local network. In many cases it is also possible to configure a timer to require re-authentication of the user.

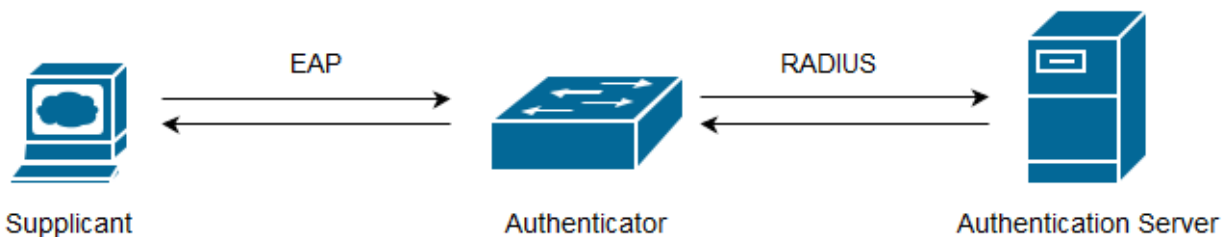


Figure 3 802.1x

The communication between the supplicant and the authenticator uses a data protocol called EAP to send credentials. It is mainly designed for serial connection, it is therefore encapsulated in an EAPOL frame (EAP over LAN). The job of EAP is to encapsulate the authentication and create an authentication method to be used between the supplicant and the authenticator. The Authenticator then re-encapsulates the method and makes it a request to the authentication server, typically the protocol RADIUS is used between the authenticator and the authentication server, but other protocols such as diameter may be used. [IDG]

802.1x authentication is no complete solution. It contains weaknesses for example if a computer is connected to a hub between the authenticator and the supplicant it will grant full access to the network from any port of the hub once the client has authenticated itself. Today, hubs are not directly common in network environments but the security risk still exist. However, you can add additional security with the help of for example IPsec, which is a framework for secure communication over an IP network. [IDG]

3.3.2 DHCP

Dynamic Host Configuration Protocol (DHCP) is a protocol that allows to dynamically assign clients in the network with an IP address. This means that clients that are enabled for DHCP retrieves all relevant network information it needs from a DHCP server on the network. DHCP is often implemented on a network server, but can also be implemented on a router or a switch. This greatly facilitates a network where each device does not have to be manually configured with a unique IP address.

IP addresses that clients retrieve are borrowed from a range of predefined IP addresses which are then handed back when not in use. This way each IP address is being used in a much more efficient manner. There are options to reserve addresses for specific devices such as servers so they always maintain the

same IP address. It is also possible to exclude IP addresses from the range of available IP addresses. [RFC2131]

When a client starts up, it sends a broadcast message and requests an IP address using a DHCP discovery packet. The DHCP server then responds with an available IP address. The client receives the offer and then sends a request with the offered IP address. Finally, the server responds to the request and allocates the IP address to that particular client. This process is often called DORA - Discover, Offer, Request and Acknowledge. [DORA]

3.3.2.1 *DHCP-Snooping*

DHCP can easily be exploited to carry out a MITM-attack. The attacker can simply connect its own DHCP server to the network. A DHCP discovery packet is a broadcast and will therefore reach all computers in the same IP segment. It is then up to the DHCP server to respond with a DHCP offer packet. The DHCP offer packet that reaches the client first is the address it will use. If then the default gateway address in the packet is the attacker's computer; all traffic from the client will travel through the attacker's computer. The attacker can then forward the traffic from the client to the original destination and thus the client will not even notice that it has been subjected to an attack. [DHCP-attack]

3.3.2.2 *DHCP rate-limit*

This function is a feature within DHCP-snooping and is used for limiting the number of DHCP packets that can come from a port, per second [CCNP-Security-Secure]. If there is not a limit on how many DHCP packets that can be sent, the DHCP address pool can easily be emptied and the clients that does not get an IP address will not be able to communicate with the rest of the network.

A client only sends two packets before it gets an IP address [DORA], so a limit on for example 10 packets per second will effectively limit this sort of attack.

3.3.3 *Port restrictions*

Port restrictions can both be limited in the number of clients that can communicate on a port at the same time, and more specifically limit which MAC addresses may communicate on the port. By limiting the number of clients that can communicate on a port, you can prevent a user from connecting a separate switch to the network or a separate wireless access point. If even higher demand for security is required, the port can be restricted to only allow certain MAC addresses. These addresses can be configured either manually or be automatically learned by the switch itself. [Port-Sec]

3.4 *Spanning Tree*

Spanning Tree is a protocol that enables building networks with multiple possible paths and still avoiding loops in the network. The protocol works at layer two of the OSI model, therefore it is about a loop free environment in the switched network. When redundant paths in the network is desirable, it may cause traffic at layer two to be passed around, creating infinite loops in the network. Spanning Tree protects against this and disables the redundant paths which is instead used as a backup link in case the active link goes down. This is automatic and no manual administration is required.

In a Spanning Tree topology there can only be one switch that is the root bridge per VLAN and will serve as a reference point when the other switches choose which ports will be open and closed. It is the switch with the lowest priority that will become the root bridge. The priority consists of the switch's

MAC address and the ID of the VLAN. The configuration of the root bridge should be done manually and shall be the switch acting as the default gateway on the subnet so that the traffic path through the network is flowing as efficiently as possible. [STP]

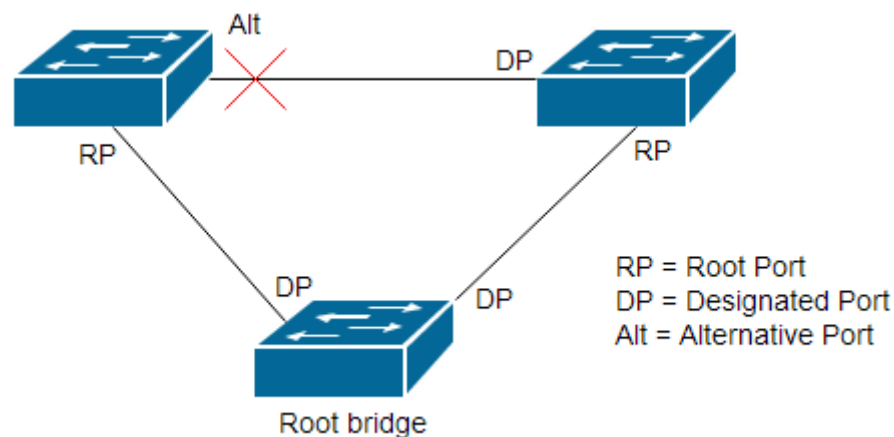


Figure 4 Spanning Tree ports

A spanning tree topology consists of different roles of the ports. The port that has the shortest path to the root bridge is called a root port. The switch serving as the root bridge is the only switch that does not have a root port. [STP]

A port is a designated port if it sends the best BPDU on its segment. On a segment there can only be one path towards the root bridge. If there is more, then there is a loop in the topology and spanning-tree disables the path that is not the root port. [STP]

A port that is neither a root port nor a designated port is a blocked port. A blocked port can be either an alternative port or a backup port. The port is an alternative if it receives better BPDUs from another bridge and backup if the BPDU was received from itself. [STP]

Spanning-tree is very slow to convergence after a change has occurred in the network topology. This means that no traffic can travel while the network converges, which is not acceptable in modern networks. This led to the Rapid Spanning Tree Protocol being recently developed to speed up this process of Spanning Tree. RSTP allows the ports to switch the status in just a second. [STP]

3.4.1 BPDU Guard

BPDU guard is a protection that is implemented on ports that are known not to receive BPDU packets, for example on access ports towards computers. BPDU guard is used as protection for outsiders not to be able to hook up a switch anywhere in the network and choose to become the root bridge, and then perform a man-in-the-middle attack (MITM) so that all traffic travels through this switch instead. Once a BPDU packet is coming in on a port where BPDU guard is enabled, the port will close so that unauthorized persons cannot plug in their own switch in any available port and execute such an attack. [BPDUguard]

3.4.2 Root Guard

The root guard is used when you want to protect a root bridge from not being taken over its role. If the root bridge receives BPDUs better than itself, they will be ignored where root guard is enabled and the port will also go down in root inconsistent state. That means no traffic will pass through this port until it ceases to send BPDUs, then the port will go up again. Root guard needs to be activated on all interfaces where you do not want another root bridge to take over. [Rootguard]

There is not much difference in BPDU guard and root guard. BPDU Guard shuts down the port completely, but root guard still allows a switch to be in the spanning-tree topology as long as it is not trying to take over as the root bridge, if so the traffic is blocked for that specific VLAN that the switch is trying to become the root bridge over. The port will automatically go up again when the connected switch ceases to send better BPDUs. [Rootguard]

3.5 Time synchronization

Time synchronization is used between the devices to have a common time between all network equipment. This is for example to facilitate the process when troubleshooting audit logs so that the time stamp of an event is showing that it occurred at the same time for all devices so that the logs gets contiguous to follow and does not vary in time between them.

3.5.1 NTP

Network Time Protocol is a protocol designed to synchronize time between different devices on the internet. NTP uses advanced algorithms for adjusting it as gently as possible in order not to affect production. NTP can simultaneously use different time references to adjust the time as accurately as possible between them, in order to deal with jitter and delay. [RFC5905]

3.5.2 SNTP

Simple Network Time Protocol (SNTP) is another protocol for synchronizing the time with. SNTP is built of exactly the same package structure as NTP has. An NTP server cannot tell the difference between a NTP and a SNTP packet. The only difference is that they handle time synchronization in different ways. SNTP is slightly simplified and lacks some of the features that NTP uses. NTP has complex algorithms to adjust and make sure that time is as accurate as possible while SNTP uses a much simpler method. SNTP also lacks the function to compare the time to multiple time references at the same time and can therefore only use one at a time. If a time reference becomes unavailable it can obviously use the next available SNTP server that is configured in a prioritized list. SNTP is best suited for smaller computers and embedded systems where NTPs complex algorithms are not needed and can take up too much memory and processing power. [SNTP]

3.5.3 Authentication

NTP has long been a protocol without authentication. Today's version of NTP does however support authentication. Authentication has become more common to use to ensure that a secure time server is being used, so that an attacker cannot consider himself to be a legitimate time server and send out invalid times. Authentication is managed using symmetric keys that must be shared in a secure manner to all clients to authenticate themselves. [RFC5905]

3.6 Audit logs

Audit logs are used to store information about various devices on an IP network. Through the logs it is then possible to see warning and error messages that have been logged. Each event is logged with a time stamp, so it is important that all devices using logs also are using time synchronization so that you can more easily track down any error messages when every device is using a common time.

3.6.1 Syslog

Syslog is a standard for data logging. It is a protocol that is used to centrally store the text messages sent from devices on the network to a single location. The point is to be able to centrally read log messages from all devices in one location instead of manually going into one device at a time and trying to troubleshoot a problem.

The protocol is simple, the syslog transmitter, which is a network device, sends a text message that is less than 1024 bytes [RFC3195] to a syslog receiver. Syslog receiver is usually called a syslog server and it runs an application that supports the syslog protocol which constantly receives these text messages and stores them.

3.7 Confidentiality

Something that is very important is to protect the data on a network device from outsiders. The configuration contains essential information about user data, passwords and other parts of how the network is structured. Especially important is to secure the access to the device by using only secure connection methods where at least a password is required. When access has been granted to the device there should be no password written in cleartext in the configuration. The configuration itself should have all passwords encrypted or hashed in order to protect their privacy from unauthorized access.

3.8 Server

A server is a computer system used to manage and administer services in a computer network for several other systems and clients. Server can also refer to a software installed as a server role on a system [ServerWiki]. All devices and computers can act as a server in some cases but it is most often referred to a more powerful and better equipped machine that is designed to perform only one function. These are usually equipped with a faster processor, more RAM, and often high storage capacity depending on what type of server it is.

3.8.1 Ubuntu

Ubuntu is a popular distribution of Linux that is completely free. It is a stable operating system with focus on ease of use. Linux is extremely scalable, making it a popular operating system for servers. You only need to install the services you need. This makes it a performance-efficient operating system that can run on most machines. It does however require some basic knowledge of Linux/Unix such as management of the terminal.

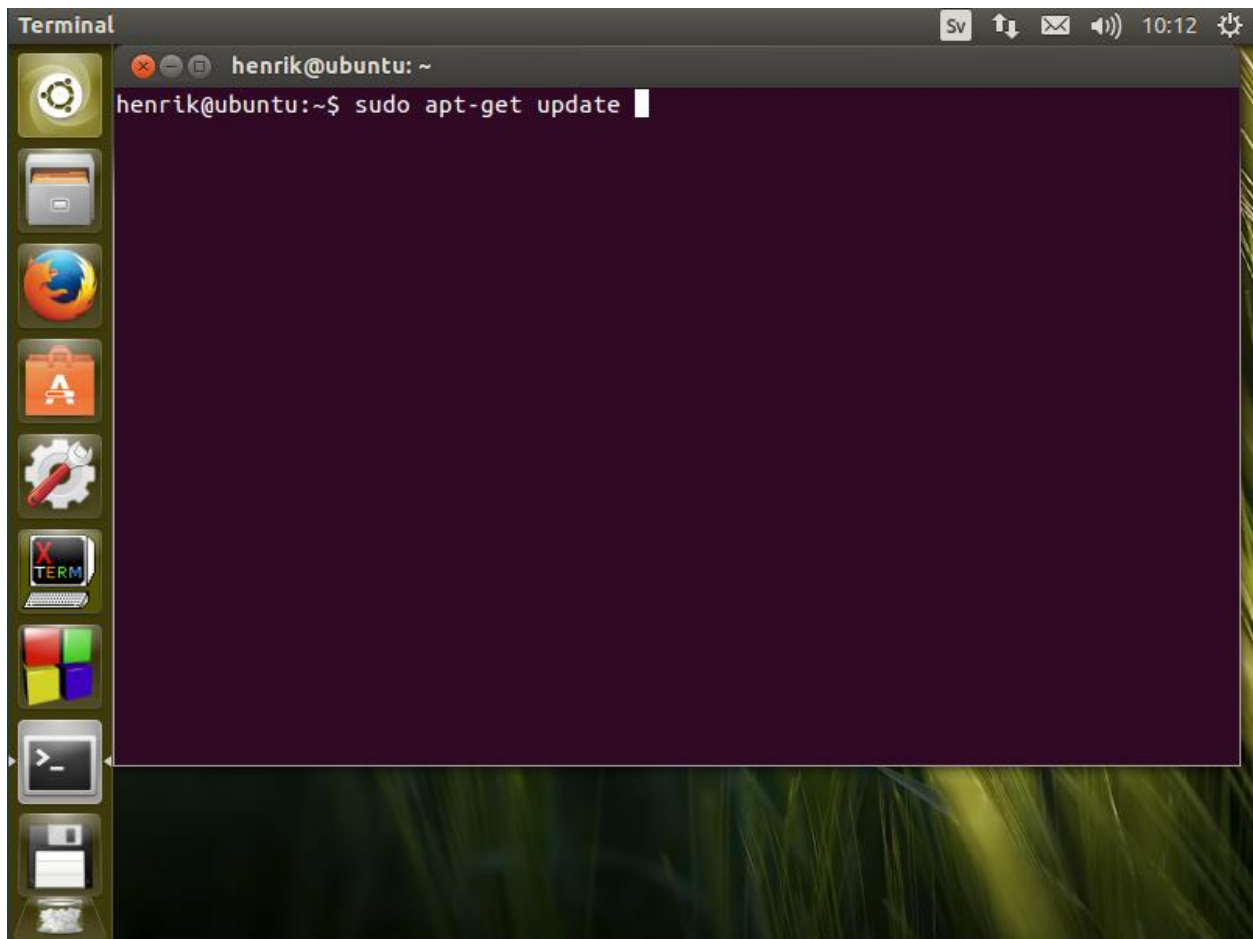


Figure 5 Ubuntu

3.8.2 Virtualization

Virtualization means that you have multiple virtual machines running on a single physical computer, this means that you can have multiple operating systems and applications running simultaneously on a single computer. This is for utilizing the performance on computers in a better way, especially on servers, and partly to use each individual virtual machine for different functions. Virtualization reduces IT costs and also saves space.

Virtual machines facilitates administration and collects everything centrally on one place. A virtual machine is very mobile in the sense that it is installed on a virtual hard drive that you can easily move around to other places. There are also features like snapshots that take an exact copy of the virtual machine so you can easily restore the machine to a previous state, much like a backup.

Applications that create and run virtual machines are called a "hypervisor" or a "virtual machine monitor". An example of such a program is VMware [VMM].

3.9 Attacks

3.9.1 Denial of Service

This type of attack is about taking up resources on the attacked unit. This typically by overloading the device with so much traffic that the device freezes or cannot handle all the valid traffic. If a system is not protected against DoS attacks it can be very easy to overload it by using scripts that generates multiple requests. A DoS attack is always done by a person or system but it can also be caused unintentional by misconfiguration or equipment failure. A DoS attack can greatly increase its influence by performing the same attack from a number of different systems directed towards a single target. This more powerful attack is referred to as a Distributed DoS (DDoS) attack [CCNP-Security-Secure]. This is something that is very difficult to protect yourself from in most cases.

3.9.2 Eavesdropping

This type of attack is aimed at eavesdropping on the traffic in a network by monitoring packets sent between systems. Then searching for sensitive information in packets consisting of passwords and other confidential information. The attack can be carried out with software that can analyze packets [OWASP]. An example of such a program is Wireshark which makes it possible to inspect packets at a microscopic level [Wireshark].

3.9.3 Man in the Middle

A "man-in-the-middle attack" is an attack that can be performed in many ways. The idea is that a malicious outsider intrudes on a communication between two parties. This allows packets from both parties who they believe are sent directly between each other actually is forwarded through the attacker, hence that person has full control over the communication between both parties. The attacker performing the MITM attack is required to be located on the same network, but the attacker is completely invisible through the communication session and have every opportunity to modify packets on their way to the receiver. MITM is an easy example of an eavesdropping attack [Techopedia]. Man-in-the-middle attack is often called MITM, MitM MIM or MIM. [Vera]

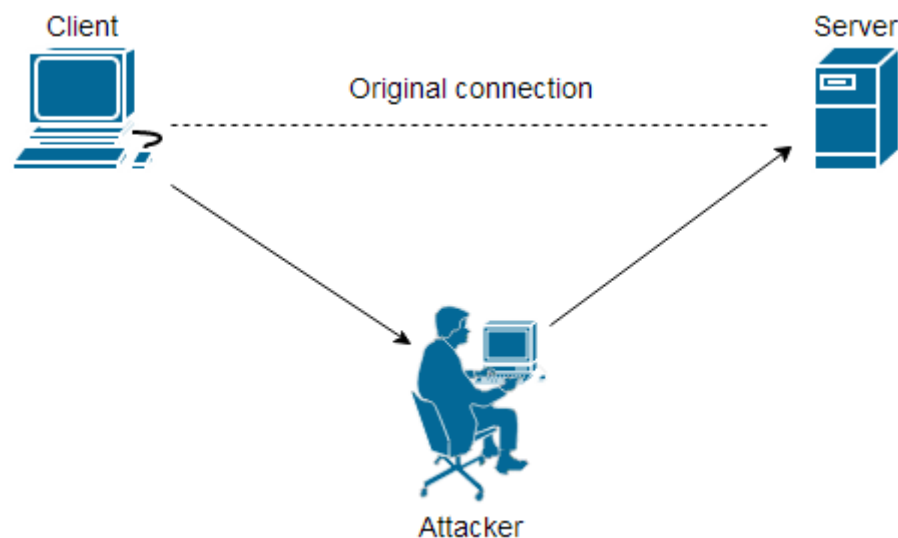


Figure 6 Man in the middle attack

3.9.4 Reconnaissance

Reconnaissance is exactly what it sounds like. It is not about performing any direct attack and perform any harm to a system or network. The purpose is to some degree have access to a system or network and then collect information about how the network looks like, what addresses are in use and which services are running on those systems within the network [CCNP-Security-Secure]. This information can then be used to perform a malicious attack after deeper knowledge how the inner network looks like. Examples of this type of attack is for example "ping sweep" which means sending pings on a whole range of addresses and finding active systems on the network. Other types of attacks are "vertical scans" and "horizontal scans" which is to scan multiple services on different port numbers on a single system respectively to scan for a specific open port or service on a full range of addresses. One example is to scan an entire range of addresses on port number 21, which is usually the service for FTP and thus find systems that have this service turned on. [CCNP-Security-Secure]

4 Thesis

ABB has a certification program for equipment that may be used together with System 800xA; Industrial IT Certification. They now want to introduce formal testing of network equipment's safety properties according to IEC 62443-3-3 and IEC 62443-4-2.

At the beginning of the thesis a lot of energy was put into studying and analyzing the new standard called IEC 62443. There were two documents from this standard that was interesting and these were 62443-3-3 and 62443-4-2. IEC 62443-3-3 describes security requirements on an entire industrial control system. IEC 62443-4-2 describes how these system requirements should be implemented in Host Devices, Applications, Embedded Devices and Network Devices.

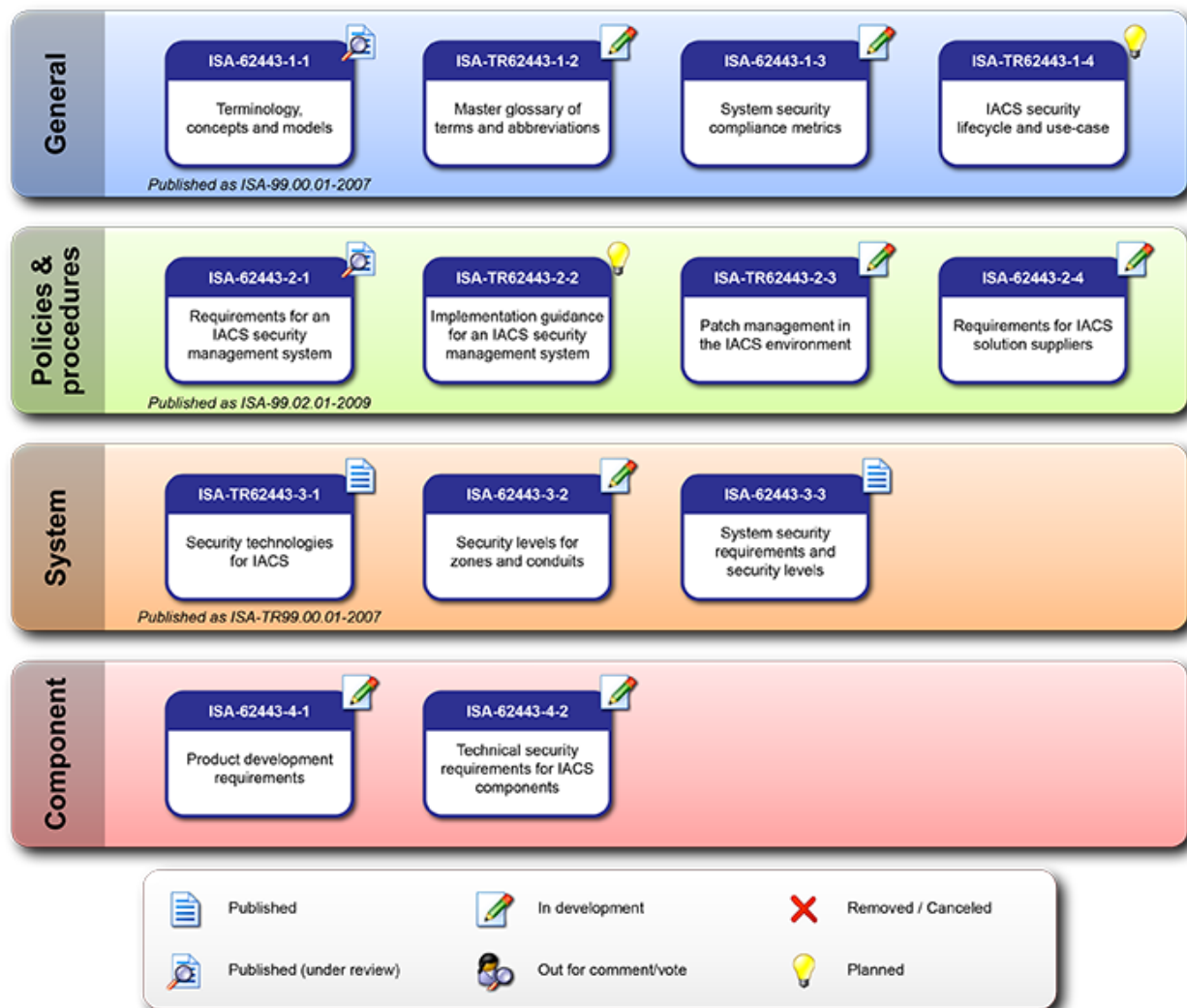


Figure 7 IEC 62443, [ISA62443]

4.1 ISA99

ISA99 is part of the International Society of Automation (ISA) and is a development committee of security experts who come from many countries around the world. This committee's purpose is to

establish standards, recommended practices, technical reports, and related information regarding safety aspects to be used for implementation and production of control systems. [ISA99]

These standards aim to improve the security and availability of components and systems used in production or control by identifying vulnerabilities and address them before they created a problem, thereby reducing the risk of confidential information falling into the wrong hands when there is a malfunction of a product. [ISA99]

ISA99's ongoing project is to create the multi-standard IEC 62443. This standard consists of a number of documents, which aims to create a comprehensive security standard. The documents content covers everything from a general level to a component level. [ISA99]

4.2 IEC 62443

During the work, two documents from the IEC 62443 standard have been used. These are IEC 62443-3-3 and IEC 62443-4-2. The information contained in IEC 62443-4-2 has been used in the first place. However, this document is not yet finished. That is when the IEC 62443-3-3 has been used since IEC 62443-4-2 is based on that document but focused on network equipment.

4.2.1 IEC 62443-3-3

This document describes the detailed technical security requirements on an entire industrial control system. The document is based on the seven fundamental requirements of IEC 62443-1-1. These requirements are:

1. Identification and authentication control.
2. Use control.
3. System integrity.
4. Data confidentiality.
5. Restrict data flow.
6. Timely response to events.
7. Resource availability.

[IEC 62443-3-3]

4.2.2 IEC 62443-4-2

This document describes how the system requirements provided in IEC 62443-3-3 should be followed in computers, applications, embedded systems and networking equipment. IEC 62443-4-2 is based on the requirements provided in IEC 62443-3-3 but focuses on components [IEC 62443-4-2]. This means that everything in IEC 62443-3-3 is not applicable and therefore not included in IEC 62443-4-2. There are also requirements in IEC 62443-4-2 that are not possible to apply on switches and therefore not all requirements of the standard have a test in the test description.

4.3 Lab room

All tests that have been made during the work has been done in the lab room at ABB. This lab room consists of a variety of network equipment, various servers and network storage for different snapshots and backups. In addition, ABB's own control system is also mounted on metal rails and are tested along with various switches for certification.

Most switches that have undergone the tests are industrial switches designed for harsh environments to withstand extreme temperature differences, dust etc. Most units also feature dual input of power for redundancy.

Before the testing of a device can be carried out, some preparation is needed. The things needed is a printed copy of the test description. It is also needed to have a printed copy of the test protocol according to the created template to record the results. It is also possible to digitally record the results directly in the document, which is also the preferred way. The equipment to be used during the test also needs to be prepared and make sure it is in working condition. One should also ensure that the switch to undergo the test is completely free from configuration and that only default factory settings are used. Subsequently, the tests are performed according to the test description that clearly describes step by step what to do and brings up preparations for each test, if any. The first time an entire test is performed it will always be more time consuming because the number of installations that need to be done, such as installing virtual servers.

The illustration below shows how a complete topology looks like during the test with all the necessary hardware needed and how it should be connected.

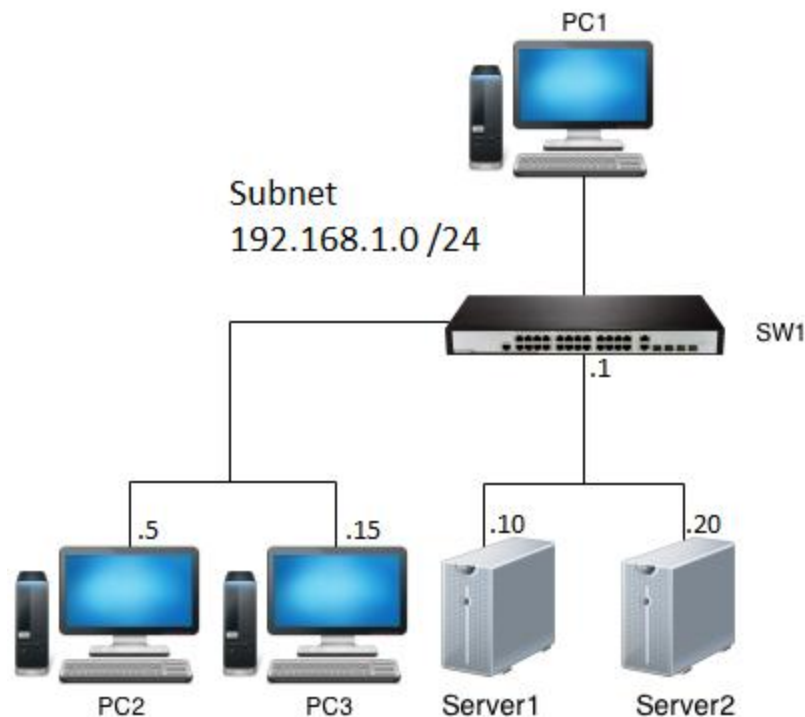


Figure 8 Lab topology

4.3.1 Equipment

Equipment used during the tests has largely consisted of borrowed hardware from ABB that was available in the lab room. In addition to the switches that have been tested there have been two desktop computers and two laptop computers used. One laptop has been used to install two virtual machines on with Ubuntu Server as the operating system. The second laptop has been used as a regular client for testing access. Both desktops have been connected to a KVM switch, meaning that they can be controlled from the same set of keyboard, mouse and monitor. It allows one to easily and quickly with the push of a button to change computers while saving room for one set of accessories for your computer. One computer has been used as a client while the other had access to the Internet and has been used to search possible problems that was encountered and also to download various programs that have been necessary. When it has been possible to use the CLI a serial to USB adapter has been used to connect to the console port on the switch.

Programs that have been used to validate and implement the tests include:

- PUTTY (beta 0.63)
Application for terminal emulation to connect to a device via either local or remote connection.
- TFTP32 4.50
Application that provides various functions like Syslog server and TFTP server.
- File Checksum Integrity Verifier
Application to generate and verify cryptographic hashes for files.
- VMware Player 6.0.2
Application to create and run virtual machines.
- Ubuntu 13.10
Distribution of Linux operating system.

VMware Player has been used to install the virtual Ubuntu servers. The necessary applications installed and used on Ubuntu servers to implement and verify the tests with are the following:

- FreeRADIUS 3.0.3 (RADIUS server)
Application that provides RADIUS for user authentication.
- snmpd (SNMP client)
Tool used for sending SNMP GET request.
- ntpd (NTP server)
Application used to synchronize the time between network devices.
- isc-dhcp-server (DHCP server)
A standardized network protocol to dynamically distribute network configuration in terms of various parameters.

4.4 Test description

During the early stages of the thesis the test description was created that all the time could be improved further as new tests were implemented. The development of the test description was done throughout the whole thesis period. The test description should be used as a general guide to assist when performing all tests on different switches to verify its compliance against the new standard in industrial data communications. As previously mentioned, the name of this standard is IEC 62443.

From this standard all the requirements was broken down into parts that are relevant and actually can be implemented on network equipment, in this case switches. Based on these requirements, the test description was created which is a detailed guide on how to test a device. Each test refers to one or more requirements of this standard. The challenge was to design different tests that could verify that these requirements were met.

The purpose of the test description was to create an easy to understand description on how to verify that a network device meets the requirements of IEC 62443-4-2. This description should be as thorough as possible to describe the purpose of the test, how to conduct the tests and what the standard say about the requirements.

Since this test description applies to several different manufacturers of switches it cannot be too in-depth but serve as a general description that addresses scenarios to test but not in great detail how to specifically do things. Specific and mandatory parts that need to be made on for example servers are however described in more detail exactly how it should be done, because that does not change.

See appendix: Product Type Test Description - Security Feature Test for Ethernet Switches.

4.4.1 Scope of use

One of ABB's key products is the control system 800xA. This control system is used to control industries, nuclear power plants, oil platforms etc. To ensure that the switches work with 800xA, ABB has a certification program that goes through a number of tests to ensure that all features in 800xA work with the switch and that the switch does not slow down the communication. After a successful certification on a switch, the manufacturer may use it together with their sale.

Recently, network security has become increasingly in demand by ABB's customers, but it is hard to know what a secure switch is. The goal of the test description is to find out what security features a switch has and finally be able to show the results for ABB's customers.

4.4.2 Structure

The name of the test description is "Security Feature test for Ethernet Switches" and is constructed according to the document "Product Type Test Description" which is a template for ABB for product testing. The document has then been adapted for this test purposes since certain titles are not applicable. These lines have been marked "Not applicable".

The headlining for each test is structured as follows.

4.4.2.1 *The purpose of the test*

All tests consist of an introduction that talks about the purpose of this test. This provides a brief explanation what the test will be about and why it is necessary to test this feature and also what type of

attack it could possibly protect against. If the test has a requirement from IEC 62443-4-2 linked to itself it is followed by a brief explanation of what is included in the requirement. If the test does not have any requirements from IEC 62443-4-2 related to itself it is followed by a longer explanation why this security feature is worth testing.

4.4.2.2 Preparation and data input

The next part is a preparation of the test, which brings up any software that needs to be installed in order to perform the test. It may include installing and configuring a RADIUS server that will later be part of the test. It may also contain a topology picture showing how the devices in the test should be addressed and connected with each other.

4.4.2.3 Procedure

A test may consist of several subtests if the test are closely related to each other. Each part consists of a numbered list of instructions that are helpful when performing the test. These instructions are detailed as much as possible but still needs to be described in general so that it fits on every possible manufacturer of switches.

4.4.2.4 Expected result

Finally, the test describes the expected results of the test. This describes besides the expected results based on each subtest, also how each test should be graded if specific requirements are set. The results of a test are generally only pass or fail, but it can also occur complications during the test and then a remark is added in the test.

4.4.3 Traceability

The majority of the tests in the test description have requirements linked to IEC 62443-4-2. This makes it possible to trace from the test to the IEC standard. In order to increase the traceability there is a summary table in the beginning of the test description with the requirements of the IEC standard and the tests related to that requirement.

There are some deviations from this and that is the tests that has no requirements from IEC 62443-4-2 linked to them. These tests have still been considered important because they prevent some common MITM, DoS and eavesdropping attacks.

As previously mentioned, there are also requirements of the IEC standard that is not covered in the test description. These have been considered as non-relevant or not applicable to a switch when the standard applies for all kinds of network equipment. It may for example be something regarding wireless network and therefore not applicable. All of these requirements is still added as traceable items in the test description followed by a motivation why they are not included in any of the tests.

4.4.4 Tests

4.4.4.1 Local account management

Account management is something that is very important. This section of the test involves examining whether it is possible, for example, to create user accounts on the device, or if you can remove the ones that come with factory settings that would usually be the username admin. To use this username increase security risks significantly as most who are trying to connect probably had guessed that username already. Most devices today are using this username as standard in default factory setting.

4.4.4.2 *Centralized account management*

Centralized account management is something that is very useful in large networks. This requirement is also something that the IEC standard demands for network equipment to be able to handle. To test the centralized login, RADIUS has been installed on two virtual Ubuntu servers. This is because in addition to testing the function, it also tests if it is possible to use redundant RADIUS servers, in case one goes down. It also includes a test to verify if it is possible to log in on a local user if no RADIUS servers are reachable.

4.4.4.3 *Local and remote connections*

The IEC standard demands that local and remote sessions should be able to be shut down manually and automatically after a configurable period of inactivity. It also includes a test where the administrator shuts down another user's connection to the switch.

4.4.4.4 *Limit connections*

Connections can be restricted in two ways: how many people that can connect simultaneously and from where they can connect. To meet the requirement of the IEC standard it is required that the limit of how many people that can connect simultaneously can be configured, which on many devices was not possible. Often the limit for the number of CLI connections was set to between one and five, and could not be changed. The number of GUI connections were on the other hand endless and could not be modified. This can be abused with ease by opening multiple connection to the switch in a browser and the performance of the switch deteriorates significantly because of this.

4.4.4.5 *Secure connection methods*

To configure a network device, you must first connect to it. A network device have often insecure connection methods enabled from the factory, such as Telnet and HTTP. But usually also have secure connection methods possible, such as SSH and HTTPS. These tests verify whether it is possible to turn off the insecure connection methods and instead enable the secure connection methods.

4.4.4.6 *SNMP*

SNMP is an insecure protocol because all information is sent unencrypted and manufacturers often use the default community strings "public" and "private" on their products. Therefore two tests are performed for SNMP version 1 and 2c which is to first see if it is possible to turn off SNMP and the second is whether it is possible to change the community strings to something other than "public" and "private".

Version 3 of SNMP uses, unlike its previous versions, both authentication and encryption and is therefore a secure protocol and should always be a prioritized over version 1 and 2c. This test verifies that SNMPv3 is present and functioning properly. In the test, authentication protocol MD5 and encryption protocol DES is used to verify its functionality, because it is supported by all SNMPv3 implementations.

Some manufacturers have made it possible to select which protocol to use. In addition to MD5 and DES, you could have the choice of SHA1 for authentication and 3DES or AES for encryption. These choices, if possible, will be recorded in the test record because they may be of interest to ABB's customers.

4.4.4.7 Audit logging

Audit is something that is needed in a network, especially when it becomes more complex as more network devices connect to the network. Then it can be difficult to keep track of each device. Audit helps when troubleshooting network problems. These tests ensure that a network device can generate their own audit logs and if possible, to send their logs to a centralized location where all logs from all network equipment is stored.

4.4.4.8 Login

Limiting the number of login attempts for users to login to the network equipment is essential. Mainly so that outsiders should not have infinitely many attempts when they try to break into the device. The tests in this section verifies if a user becomes locked after too many invalid attempts and if this number can be limited. One of the tests checks, among other things, if invalid login attempts are logged. This can be good to see the specific usernames possibly at risk.

Tests include to see if the device can display a message at login via both CLI and GUI to warn whom the device belong to and warn that unauthorized access is prohibited.

4.4.4.9 Time

This test verifies if it is possible to change the time and date on the network equipment manually or by using a NTP server. The NTP server has been one of the Ubuntu servers that have been available during the tests.

A test was also including to authenticate the NTP server with symmetric keys. This test however, was difficult to carry out because the NTP server in Ubuntu does not support authentication and no other free software either.

4.4.4.10 DHCP

DHCP is an easy target for a MITM attack or a DoS attack so therefore has the security function DHCP snooping and DHCP rate-limit been included in the test description, although it was not possible to link these tests to a requirement of the IEC standard. However ABB, together with other industrial communication equipment manufacturers, does not use DHCP in their industrial environment. Perhaps since static IP addresses are often used, this is not mentioned in the standard.

To test DHCP snooping the switch has been configured to not trust any DHCP server on any port. Then the DHCP server is connected, which is installed on one of the virtual Ubuntu servers. When one of the clients then asks for an IP address the client will not get an IP address assigned, because the switch will block this package or shut down the port.

DHCP rate-limit has been tested by configuring the limit on the number of packets per second to as low value as possible, usually between 0 and 1 on the switches that have been tested. One client connected to the port of the switch have then been asking for an IP address from the DHCP server. Because a client sends two packets to get an IP address, the limit will be exceeded.

4.4.4.11 Port security against users

Since many attacks occur from ports that are locally connected to the users themselves within the organization, it is important to restrict even these ports. Access from these ports are of course a much

easier option for an unauthorized person to gain access to vulnerable data compared to accessing the data from outside the organizations local network.

Port-based authentication, 802.1x is something that increases the security requirements of a network. It requires that each client that connects to the network need to enter additional information in term of a username and a password to authenticate to the network. This prevents anyone from connecting a computer directly and granting them full access. It can also be configured so that authentication needs to be renewed after a certain period of time if desired.

It is recommended to secure the port and restrict so that only one user have access to it when it is known that only one client will be connected to that access port. Alternatively, to limit the port to allow only a specific MAC address. Both of these methods are included in this test.

4.4.4.12 Network segmentation

A basic function of the switches is to segment the network in different virtual networks (VLAN). This function is also a requirement of IEC 62443-4-2 and is verified by a test. The test verifies that computers within the same VLAN can communicate with each other, while they cannot communicate with computers outside their own VLAN. VLANs are not primarily implemented because of security reasons. Its main use is to restrict broadcast traffic from effecting too many computers in the network. [VLANs]

4.4.4.13 Backup of configuration file

In order to quickly replace a switch when a fault has been detected, it is great if the configuration file from the previous switch is available to quickly get the new switch in use. The backup process is divided into three different tests where the first test verifies whether it is possible to download the configuration file either with a file transfer program such as TFTP or save it directly to the local computer.

The second test verifies whether it is possible to automate the backup process. This can be good if there is a larger network or if changes are made continuously since it can be forgotten.

The third test verifies if it is possible to load a saved configuration back on the switch and use it.

4.4.4.14 Spanning Tree

For spanning tree two tests are carried out, one tests BPDU guard and the other tests root guard. These tests along with the tests for DHCP snooping and rate-limit is the only ones that has no requirements of the IEC standard linked to them, but was chosen to be included anyway, since it by simple means can gain access to information or conducting a DoS attack by manipulating BPDU packets.

To test BPDU guard the switch was connected with another switch that also uses spanning tree. After BPDU guard is enabled, the port should somehow get blocked, so that traffic from the second switch cannot reach the device under test.

Root guard is also tested by connecting another switch. The switch under test will begin with having a lower priority than the second switch, making sure it is the root bridge. After that root guard is enabled, everything should still work. Once it has been verified that everything works as it should the priority is changed on the second switch so that it has lower priority than the switch under test, this will make it

attempt to become the root bridge. If root guard is functioning properly, the port will end up in a root-inconsistent state and the switch will not drop its root bridge status.

4.4.4.15 Confidentiality

Protecting sensitive data is something that quite often is relevant. In this case, it is about ensuring that all passwords in the configuration are encrypted and not written in cleartext. It also applies to verify that the configuration or software is unchanged before they are imported into the system.

4.5 Test record

For the test description a test record has been created as a template to record all the results from the tests in. One test record is required per unit and test. These tests have been conducted on various selected switches from the lab room at ABB with mixed manufactures. It is devices from Cisco and HP to more specialized industrial brands such as the German brand Harting and Weidmüller. For all tests in the test record it has been noted the steps taken to proceed the test. If the CLI was used during the test these commands has been written down, but some of these devices had only had a graphical interface and then it has also been written down in detail where to navigate in the menus and what setting that needs to be made for each step.

After each completed test the switch is graded based on the result. The different results are passed, failed, passed with remark, failed with remark, not applicable and not tested.

A remark can be given when the result of the test is not as expected. Some tests have been given the results passed with remark when the switch does not fulfill all the requirements of the IEC standard, but it meets the requirements that are considered to be important. These special cases how each test should be graded is also noted in the expected result section of the test description.

Failed with remark can be given when the switch claims to support a function, but the result of the test indicate that the function does not work. This can occur when there is a bug in the switch's software, which also occurred during the tests that have been carried out.

The test record is designed after an ABB template called "Product Type Test Record". The template has several purposes for different types of tests. The title of the test record is "Security Feature Test for Ethernet Switches" followed by the brand and model of the device under test that is manually filed in.

See appendix: Product Type Test Record - Security Feature Test for Ethernet Switches - Cisco IE 3000-8TC

4.6 Comparison chart

Based on the results of the tests from the test description, an easy to understand comparison was created that clearly shows how secure an individual switch is compared to others. This comparison was one of the original goals of the project and will be available for ABB's customers when they will choose brand of switch to be purchased to their network.

This type of comparison is not normally done at ABB, so the design and layout of the comparison was free for interpretation. Several suggestions for the final comparison were made and later reviewed by the involved employees at ABB. They have then been able to choose the one they think is best represented.

Finally a design was chosen consisting of a combination of two different comparisons. On the top of the page the switch is presented with a picture, name and what software was used during the test. Below it is a pie chart diagram that gives the reader an idea of how much the switch is capable of, in percentage. Then comes the next part that consists of a complete list of all tests with a brief explanation. In case of a passed test the switch has a green check mark next to it and in case of a failed result, it has a red cross. If the test is not carried out for some reason it is left empty. The results of the switches are stacked next to each other so that you can quickly compare the switches security features against each other.

See appendix: Comparison chart

5 Conclusion

We have developed a structured test to effectively verify the security features a switch has implemented. The results of the tests show that there is a big difference between different manufacturers. In general, regular desktop switches has much more security features implemented than industrial switches, with some exceptions.

This test description is designed after a new security standard within industrial data communications. The tests are not interesting if you only perform them on a single device with the belief that the unit will pass of all the different tests, because this is not likely. The results starts to get interesting when the tests are carried out on a variety of devices and when you can compare the different results among them.

The comparison chart can also be advantageous for the environment because ABB's customers may be much more likely to choose the switch that fits their needs from a security perspective and thus will not result in the company having to purchase new switches if the first purchased ones did not meet their requirements.

Comparing the prices among the tested switches, gives an indication that slightly more lavish switches are capable of more security requirement, but that is not always true. From a security point of view, the little more costly devices have additional security features but that may not always be something that everyone takes advantage of in their network. Do we really need all the features of the most expensive switches? It is an important question you should ask yourself before purchasing new equipment. The choice depends on where in the network the device will be located and what purpose it should fulfill. Small industrial switches may not have some features you may think are very critical, such as secure connection method.

IEC 62443-4-2 and IEC 62443-3-3 gives cause to very loose interpretation of the requirements because they are very general for all kinds of network equipment. Requirements are rarely constructed so that it is actually possible to fulfill them. Instead you may come up with a test and then try to match it to a requirement by reading the description. ABB does not generally believe that certification is particularly useful, because new features are continuously released, creating new vulnerabilities that were not included by the certification.

5.1 Future work

Suggestions for improvements could have been to continue develop the test description with additional tests for requirements from the standard document that was missing in the test description. After a

meeting, we concluded that some of requirements from the IEC 62443-4-2 is possible to design additional tests for. This include for example "Emergency power" as one of the requirements specified by the standard. It is about being able to have redundant power supply. It is something that belongs to the hardware and therefore no test has been designed for it since the focus was on security features in switches software. But there is obviously a suggestion for improvement for future development of the test description.

The thesis focused on software security features of switches. No tests have thus been implemented on the switch hardware because it is not included in the standard document. However, it was wishes from ABB to have complementary documents with these physical tests. ABB has a machine particularly used for robustness testing, called Achilles Test Platform, but there was no time left to learn how Achilles works. These tests had in this case been separate from the test description. Achilles can perform various types of load tests and "fuzz testing" which involves manipulating the data of the packet and send invalid and unexpected data to the device under test to see how it reacts. Nor how well it manages a penetration test has been performed.

6 References

6.1 IEC 62443

[IEC 62443-3-3] ISA-62443-3-3 Security for industrial automation and control systems Part 3-3: System security requirements and security levels

<http://isa99.isa.org/Documents/Drafts/ISA-62443-3-3-WD.pdf>, Published January 2013 Draft 4, Retrieved 2014-06-11 (During the project the final document has been used, but it is not available on the internet).

[IEC 62443-4-2] ISA-62443-4-2 Security for industrial automation and control systems Part 4-2: Technical Security Requirements for IACS Components

<http://isa99.isa.org/Documents/Drafts/ISA-62443-4-2-WD.pdf>, Published Mars 2011 Draft 1, Retrieved 2014-06-10 (During the project a later draft has been used, published 2013-08-14, but it is not available on the internet).

6.2 Books

[CCNP-Security-Secure] Sean Wilkins & Trey Smith, "CCNP Security Secure 642-637 Official Certification Guide", pages 31-35 & 76 & 257, 2011.

[DATAKOM] Valentino Berti & Mats Björkman & Lars-Åke Nordén & Anders Lindgren, "Datakommunikation", pages 227-230, 2012.

[COMP-GUIDE] Cisco Networking Academy, "Routing and Switching Essentials Companion Guide", 2014.

[SWITCH] Richard E. Froom, "Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide: Foundation Learning Guide for SWITCH 642-813", 2011.

6.3 Internet references

6.3.1 Cisco documentation

[TACACS+vsRADIUS] "TACACS+ and RADIUS Comparison",

<http://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html>, Last edited 2008-01-14, Retrieved 2014-06-03.

[BPDUguard] "Spanning Tree PortFast BPDU Guard Enhancement",

<http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10586-65.html>, Last edited 2005-09-01, Retrieved 2014-06-09.

[HARDEN] Shashank Singh, "Cisco Guide to Harden Cisco IOS Devices",

<http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html#anc39>, Last edited 2014-01-03, Retrieved 2014-07-08.

[Rootguard] "Spanning Tree Protocol Root Guard Enhancement",

<http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10588-74.html>, Last edited 2005-08-30, Retrieved 2014-06-09.

[Cisco8021x] Cisco Configuration Guide, "Configuring IEEE 802.1x Port-Based Authentication", http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/sw8021x.pdf, Retrieved 2014-06-03.

[STP] "Understanding Rapid Spanning Tree Protocol (802.1W)", <http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24062-146.html>, Last edited 2014-10-24, Retrieved 2014-06-03.

[DHCP-attack-cisco] Kevin Lauerman & Jeff King, "DHCP Consumption Attack and Mitigation Techniques White paper", http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/white_Paper_C11_603833.html, Retrieved 2014-07-01.

[Port-Sec] Cisco Configuration Guide, "Port Security", http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/port_sec.html#wp1071035, Retrieved 2014-07-09.

[VLANs] Stephen McQuerry, "CCNA Self-Study (ICND Exam): Extending Switches Networks with Virtual LANs", <http://www.ciscopress.com/articles/article.asp?p=102157>, Retrieved 2014-08-12.

6.3.2 RFC

[RFC2131] RFC 2131, "Dynamic Host Configuration Protocol", <http://www.ietf.org/rfc/rfc2131>, Published 1997-03, Retrieved 2014-06-02.

[RFC2574] RFC 2574, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", <http://www.ietf.org/rfc/rfc2574.txt>, Published 1999-04, Retrieved 2014-06-04.

[RFC2616] RFC 2616, "Hypertext Transfer Protocol -- HTTP/1.1", <https://tools.ietf.org/html/rfc2616>, Published 1999-06, Retrieved 2014-07-09.

[RFC3195] RFC 3195, "Reliable Delivery for syslog", <http://tools.ietf.org/html/rfc3195>, Published 2001-11, Retrieved 2014-06-09

[RFC4253] RFC 4253, "The Secure Shell (SSH) Transport Layer Protocol", <http://tools.ietf.org/html/rfc4253>, Published 2006-01, Retrieved 2014-07-09.

[RFC5905] RFC 5905, "Network Time Protocol Version 4: Protocol and Algorithms Specification", <http://www.ietf.org/rfc/rfc5905.txt>, Published 2010-06, Retrieved 2014-06-04.

6.3.3 Other internet references

[SNMP] SNMP, "Extended Security Options", <http://www.snmp.com/protocol/eso.shtml>, Retrieved 2014-06-04.

[NET-SNMP] "Net-SNMP", <http://www.net-snmp.org/>, Retrieved 2014-07-09.

[ISA99] ISA99, "ISA99, Industrial Automation and Control Systems Security", <https://www.isa.org/isa99/>, Retrieved 2014-06-11.

[Wireshark] Wireshark, "About Wireshark",
<http://www.wireshark.org/about.html>, Retrieved 2014-07-04.

[IANA] IANA, "Internet Assigned Numbers Authority",
<http://www.iana.org>, Retrieved 2014-07-07.

[DORA] "DHCP Dora process",
<http://thetechnologychronicle.blogspot.se/2013/08/dhcp-dora-process.html>, Published 2013-08-05,
Retrieved 2014-06-02.

[IDG] Mikael Simovitz, "802.1x Lämnar inga lösa trådar",
<http://techworld.idg.se/2.2524/1.410733/8021x-lamnar-inga-losa-tradar/>, Published 2011-11-01,
Retrieved 2014-06-03.

[VMM] Wikipedia, "Hypervisor",
<http://en.wikipedia.org/wiki/Hypervisor>, Retrieved 2014-06-02.

[ServerWiki] Wikipedia, "Server (computing)",
[http://en.wikipedia.org/wiki/Server_\(computing\)](http://en.wikipedia.org/wiki/Server_(computing)), Retrieved 2014-06-02.

[DoS-atk] Wikipedia, "Denial-of-Service attack",
http://en.wikipedia.org/wiki/Denial-of-service_attack, Retrieved 2014-07-02.

[SNTP] Time Tools, "The Difference Between NTP and SNTP",
<http://www.timetools.co.uk/2013/07/23/the-difference-between-ntp-and-sntp-protocols/>, Published
2013-07-23, Retrieved 2014-06-09.

[DHCP-attack] Telelink, "DHCP attacks",
<http://itsecurity.telelink.com/dhcp-attacks/>, Retrieved 2014-07-01.

[HTTPS] Microsoft TechNet, "What is TLS/SSL?",
<http://technet.microsoft.com/en-us/library/cc784450%28v=ws.10%29.aspx>, Retrieved 2014-07-10.

[Techopedia] Cory Janssen, "Man-in-the-middle Attack (MITM)",
<http://www.techopedia.com/definition/4018/man-in-the-middle-attack-mitm>, Retrieved 2014-07-03.

[Vera] Neil duPaul, "Man in the Middle Attack",
<http://www.veracode.com/security/man-middle-attack>, Retrieved 2014-07-03

[OWASP] OWASP, "Network Eavesdropping",
https://www.owasp.org/index.php/Network_Eavesdropping, Last edited 2012-08-10, Retrieved 2014-
07-04.

[ISA62443] Gilsinnj "ISA-62443 Standard Series 2012" – Own work previously published: ISA99 Standards
Committee
http://upload.wikimedia.org/wikipedia/commons/9/97/ISA-62443_Standard_Series_2012.png,
Retrieved 2014-06-05

[ArsTechnica] Sean Gallagher, “When passwords attack: The problem with aggressive password policies”, <http://arstechnica.com/business/2011/10/when-passwords-attack-the-problem-with-aggressive-password-policies>, Published 2011-10-31, Retrieved 2014-07-21.

[MicrosoftPasswordPolicy] “Password Policy”, [http://technet.microsoft.com/en-us/library/hh994572\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/hh994572(WS.10).aspx), Last edited 2012-10-23, Retrieved 2014-07-22.

7 Appendices

7.1 Mail interview

Stefan Willby, IIT Certification Engineer, Control Technologies, ABB

Which department do you work at?

PACT XAAI

What's 800xA and what is it used for?

System 800xA's 'xA' stands for Extended Automation and utilizes the system architecture which was built for application integration in a fully redundant, reliable environment. System 800xA extends the reach of traditional automation systems - beyond control of the process - to increase energy efficiency, asset utilization, energy savings and operator effectiveness.

Why do ABB certify switches?

The certification process applies to those products and solutions that are interoperable with 800xA and provide the "plug and produce" functionality that helps customers achieve lower total cost of ownership. Certification is focused on integration and usability - installation, documentation and operation. It verifies performance with respect to System 800xA, i.e. non-interference with 800xA operation.

The benefits of certification for vendors:

- Industrial IT Enabled Certificate issued by ABB
- The certificate can be used in marketing activities
- The certificate will be published on ABB's internal and external websites
- Industrial IT Enabled Symbol available to vendor
- The Symbol can be used in marketing activities
- The symbol can be used on product packaging or documentation

Benefits for end customers:

- A product that is already tested and known to work in an 800xA environment
- A product that can be supervised, via SNMP, by 800xA (managed products only)
- A wider range of integrated 3:rd party products suited for their specific needs

Benefits for ABB:

- We extend our offering to end customers with integrated 3rd party products and their respective functionality.

Describe the whole certification process.

Network components includes 3rd party hardware that is used as a base for System 800xA (infrastructure equipment). Right now we focus mainly on switches and routers.

The following checkpoints applies (switches):

1. It should be possible to integrate the device into PC, Network and Software Monitoring (PNSM) via SNMP. (managed switches)
2. RNRP* Multicast traffic must work properly
3. High load in the switch must not violate the redundancy supervision (RNRP* multicast)
4. The switch must be able to handle fast switches of Ethernet (MAC) addresses (redundant controllers).
5. Controllers connected with half duplex must not get any Ethernet interface errors: CRC errors, framing errors, Lost Carrier sense or collisions.
6. It must be possible to deactivate IGMP snooping.
7. It must be possible to configure transmission mode and speed on managed switches.
8. Power failure and power-up must be handled accurate and not create unnecessary status changes in the communication.
9. High load or internal delays in the switch must not introduce a transmission delay that violates the time accuracy.
10. Auxiliary contact for reporting of summary failure including power failure should exist.
11. Impact of CPU switching on switch supervision.

*RNRP: Redundant Network Routing Protocol

How will our test description come in use?

IIT certification strives to expand the offering. Many customers are starting to asking for security in control systems. We therefore felt it was appropriate to develop a safety test. The results will give the costumers an overview of what security features the IIT certified products have.

7.2 Comparison chart

					
	Cisco IE3000-8TC S-IPSERVICESK9-M version 15.0(2)SF	DELL PowerConnect 7024 4.2.2.3	Hirschmann RSP 25 HIOS-25-PRP-02.0.01	DELL PowerConnect 3524	HP A3600 5.20.99 release 2101P01
					
1 Account management					
1.1.1 Add user accounts	✓	✓	✓	✓	✓
1.1.2 Remove user accounts	✓	✓	✓	✓	✓
1.1.3 Remove preconfigured user accounts	✓	✓	✓	✓	✓
1.1.4 Activate/Disable user accounts	✗	✓	✓	✗	✗
1.2.1 Handle authentication on centralized server	✓	✓	✓	✗	✗
1.2.2 Local database as backup if centralized authentication-server fails	✓	✓	✓	✓	✓
1.2.3 Redundant centralized authentication-servers	✓	✓	✓	✓	✓
1.3 Force a certain strength on new passwords	✓	✓	✓	✓	✓
1.4.1 User accounts with different privileges	✓	✓	✓	✓	✓
1.4.2 Create custom made privileges	✓	✗	✗	✗	✗
2 Sessions					
2.1 Automatically terminate local sessions after a time-period	✓	✓	✓	✓	✓
2.2.1 Automatically terminate remote sessions after a time-period	✓	✓	✓	✓	✓
2.2.2 Terminate another users connection	✓	✓	✗	✗	✓
2.3.1 Disable SNMP	✓	✓	✓	✓	✓
2.3.2 Change default SNMP community-string	✓	✓	✓	✓	✓
2.4 SNMPv3	✓	✓	✓	✓	✓
2.5.1 Confine HTTP/HTTPS connections to a certain IP-address/subnet	✓	✓	✓	✓	✓
2.5.2 Confine Telnet/SSH connections to a certain IP-address/subnet	✓	✓	✓	✓	✓
2.5.3 Confine SNMP-requests to a certain IP-address/subnet	✓	✓	✓	✓	✓
2.6.1 Limit concurrent Telnet/SSH connections	✓	✓	✓	✓	✓
2.6.2 Limit concurrent HTTP/HTTPS connections	✗	✗	✗	✗	✗
2.7.1 SSH	✓	✓	✓	✓	✓
2.7.2 HTTPS	✓	✓	✓	✓	✓
2.7.3 Disable Telnet	✓	✓	✓	✓	✓
2.7.4 Disable HTTP	✓	✓	✓	✓	✓
3 Audit					
3.1.1 Create and save audit-logs on local switch	✓	✓	✓	✓	✓
3.1.2 Create and send audit-logs to centralized server	✓	✓	✓	✓	✓
3.1.3 Change level of information logged	✓	✓	✓	✓	✗
4 Login					
4.1.1 Lock a user after a number of unsuccessful login attempts	✓	✓	✓	✓	✗
4.1.2 Unlock locked user	✓	✓	✓	✓	✗
4.1.3 Create log event on unsuccessful login attempts	✓	✓	✓	✓	✓
4.2.1 System use notification CLI	✓	✓	✓	✓	✓
4.2.2 System use notification GUI	✗	✗	✓	✗	✓
5 Time					
5.1.1 Change the time manually	✓	✓	✓	✓	✓
5.1.2 Change the time using NTP	✓	✓	✗	✓	✓
5.2 Authenticate the NTP-server	✓	✓	✗	✓	✓
6 Port security general					
6.1 Manually shut down a port	✓	✓	✓	✓	✓
6.2 Protect against rogue DHCP-servers	✗	✓	✗	✓	✓
6.3 Implement DHCP-rate-limit	✗	✓	✗	✗	✗
7 Port security against users					
7.1 802.1x	✓	✓	✓	✓	✓
7.2.1 Set a maximum number of users that can communicate on a single port	✓	✓	✓	✓	✓
7.2.2 Set what MAC-addresses can communicate on a single port	✓	✗	✓	✗	✓
8 Other functionality					
8.1 Logically segment the network using VLANs	✓	✓	✓	✓	✓
8.2.1 Manually backup the configuration-file	✓	✗	✗	✗	✓
8.2.2 Automated backup of configuration file.	✓	✗	✗	✗	✓
8.3 Block BPDUs on access-ports	✓	✓	✓	✓	✓
8.4 Protect the root switch in a spanning-tree topology	✓	✓	✓	✓	✓
9 Confidentiality					
9.1 Encrypt passwords in the configuration file	✓	✓	✓	✓	✓
9.2.1 Compute MD5/SHA1 checksum on configuration-file	✓	✗	✗	✗	✗
9.2.2 Compute MD5/SHA1 checksum on firmware	✓	✗	✗	✗	✗



Security Feature Test for Ethernet Switches

Product Type Test Description

Type des.	Part no.				
Prep. / William Kvarnström	2014-06-27	Doc. kind Title Security Feature Test for Ethernet Switches	No. of p. 45		
Appr. /					
Resp. dept	Draft				
	ABB AB	Doc. no.	Lang.	Rev. ind.	Page
		3BSE079920	en		1

1	INTRODUCTION	4
2	REFERENCES	4
2.1	Related Documents.....	4
2.2	Input Documents	4
3	TERMINOLOGY	4
4	CONFORMITY WITH REQUIREMENTS SPECIFICATION	5
5	THE SCOPE OF THE PRODUCT TYPE TEST	7
6	PRODUCTION OF THE ITEM TO BE TESTED.....	7
7	TEST EQUIPMENT	7
7.1	Software configuration.....	8
7.2	Hardware configuration	8
7.3	Auxiliary Software for the test.....	8
7.4	Tools	9
7.5	Connection Method	9
7.6	Install Ubuntu 13.10 virtually	10
8	TEST PROCEDURES	14
8.1	1 - Account Management	14
8.1.1	1.1 User accounts.....	14
8.1.2	1.2 Centralized authentication	15
8.1.3	1.3 Strength of password	19
8.1.4	1.4 User account privileges.....	20
8.2	2 - Sessions	21
8.2.1	2.1 Local sessions	21
8.2.2	2.2 Remote sessions	21
8.2.3	2.3 SNMP	22
8.2.4	2.4 SNMPv3	24
8.2.5	2.5 Confine connections	25
8.2.6	2.6 Limit concurrent connections	26
8.2.7	2.7 Secure connection methods.....	27
8.3	3 - Audit.....	28
8.3.1	3.1 Create audit-logs	28
8.4	4 - Login	30
8.4.1	4.1 Unsuccessful login attempts	30
8.4.2	4.2 System use notification	31
8.5	5 - Time.....	32
8.5.1	5.1 Change time	32
8.5.2	5.2 Authentication	33
8.6	6 - Port security general	34
8.6.1	6.1 Manual shutdown.....	34
8.6.2	6.2 Rogue DHCP-server	34
8.6.3	6.3 DHCP rate limit.....	36
8.7	7 - Port security against users	37
8.7.1	7.1 802.1x.....	37
8.7.2	7.2 Port restrictions.....	38
8.8	8 - Other functionality	40
8.8.1	8.1 Network segmentation	40
8.8.2	8.2 Backup	41
8.8.3	8.3 Spanning-tree – block BPDUs	42
8.8.4	8.4 Spanning-tree – protect the root switch.....	42
8.9	9 - Confidentiality.....	43

8.9.1	9.1 Encrypt passwords	43
8.9.2	9.2 Integrity check	44
9	APPENDICES	45

1 INTRODUCTION

This document defines the procedures for the Security Feature Test for Ethernet switches.

These tests are based on the security demands that IEC 62443-4-2-document describes. IEC 62443-4-2 describes how the security requirements from IEC 62443-3-3 should be implemented in host devices, applications, imbedded systems and network devices.

2 REFERENCES

2.1 Related Documents

Ref.	Identity	Title
[Re1]	3BSE038909	Test Process
[Re2]	3BSE025248	Product Type Test Process, PTT
[Re3]	3BSE028024	Checklist for reviews
[Re4]	3BSE039243	Terminology Document
[Re5]	3BSE080082	Product Type Test Record
[Re6]	IEC 62443-3-3	Industrial communication networks – Network and system security – Part 3-3: System security and security levels
[Re7]	IEC 62443-4-2	Security for industrial automation and control systems Technical Security Requirements for IACS Components

2.2 Input Documents

Not applicable.

3 TERMINOLOGY

All general terms are listed in Terminology Document [Re4].

Term	Definition
CAM	Content Addressable Memory
CLI	Command Line Interface
DES	Data Encryption Standard
DoS	Denial of Service
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
MD5	Message-Digest algorithm 5
MIB	Management information base
NIC	Network Interface Card
NTP	Network Time Protocol
PC	Personal computer
RADIUS	Remote Authentication Dial-in User Services
SFTP	SSH File Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell

4 CONFORMITY WITH REQUIREMENTS SPECIFICATION

The following product requirements are specified in IEC 62443-4-2 [Re7] and are verified by test cases in this document.

Req. ID	Headline	Test No.
NCR 1.1	Human user, process and device identification and authentication	1.1, 2.1, 7.1
NCR 1.2	Software process and device identification and authentication	5.2
NCR 1.3	Account management	1.1, 1.2
NCR 1.4	Identifier management	1.2, 7.1
NCR 1.5	Authenticator management	1.1
NCR 1.7	Strength of password-based authentication Requirement	1.3
NCR 1.11	Unsuccessful login attempts	4.1
NCR 1.12	System use notification	4.2
NCR 1.13	Access via untrusted networks	2.5, 2.7
NCR 1.14	Strength of symmetric key authentication	9.1
NCR 2.1	Authorization enforcement	1.4
NCR 2.5	Session lock	2.2
NCR 2.6	Remote session termination	2.2
NCR 2.7	Concurrent session control	2.6
NCR 2.8	Auditable events	3.1
NCR 2.9	Audit storage capacity	3.1
NCR 2.11	Timestamps	3.1, 5.1
NCR 3.1	Communication integrity	2.7
NCR 3.4	Software and information integrity	9.2
NCR 3.7	Session integrity	2.7
NCR 4.1	Information confidentiality	2.4, 2.7
NCR 4.3	Use of cryptography.	2.7
NCR 5.1	Network segmentation.	8.1
NCR 6.1	Audit log accessibility	3.1
NCR 7.1	Denial of service protection	6.2, 6.3, 7.2
NCR 7.2	Resource management	2.5, 2.6
NCR 7.3	Control system backup	8.2
NCR 7.4	Control system recovery and reconstitution	8.2
NCR 7.7	Least functionality	2.3, 6.1

The following tests are missing reference to IEC 62443-4-2 [Re7] but fulfills an important case.

Test No.	Subject	Motivation
6.2	DHCP-server	Mitigates Man-in-the-Middle attacks with the use of a rogue DHCP-server.
8.3, 8.4	Spanning-tree	Protect the network against privilege escalation and Man-in-the-Middle attacks with attacks against the spanning-tree topology.

The following product requirements from IEC 62443-4-2 [Re7] are not verified by test cases in this document with the motivation that follows.

Req. ID	Headline	Motivation
NCR 1.6	Wireless access management requirement	A switch itself does not provide wireless access and because a switch does not inspect traffic it cannot know if the device communicating through it is connected through a wireless access point.
NCR 1.8	Public key infrastructure certificates requirement	Certificates are too complex for this type of test description.
NCR 1.9	Strength of public key authentication	Certificates are too complex for this type of test description.
NCR 1.10	Authenticator feedback	Showing asterisks instead of the password is too obvious to be tested.
NCR 2.2	Wireless use control	A switch itself does not provide wireless access.
NCR 2.3	Use control for portable and mobile devices	A switch does not inspect traffic and can therefore not know if the device communicating through it is portable.
NCR 2.4	Mobile code	A switch cannot have installed software on them.
NCR 2.10	Response to audit processing failures	Audit logs are generally sent to a centralized server using Syslog. Therefore the server handles the errors.
NCR 2.12	Non-Repudiation	Not applicable because only administrators should be able to configure a switch.
NCR 3.2	Malicious code protection	A switch does not inspect traffic and will therefore not detect if the traffic sent through it is malicious.
NCR 3.3	Security functionality verification	A switch does not support maintenance tests on itself.
NCR 3.5	Input validation	Not testable because it requires the person that is testing to test every writable command on a switch.

NCR 3.6	Error handling	Not testable because it requires that the test should make the switch create error messages.
NCR 3.8	Protection of audit information	To connect to a switch you need to authenticate. Before that you cannot do anything.
NCR 3.9	Originality	This function has never been seen on a switch.
NCR 4.2	Information persistence	This requires the tester to know every command that uses a password and see if it can be encrypted.
NCR 5.2	Zone boundary protection	Not applicable because switches resides in the local network, therefore no zones exists.
NCR 5.3	General purpose person-to-person communication restrictions	Switches does not inspect traffic and can therefore not differentiate between different streams of traffic.
NCR 5.4	Application partitioning	Partitioning is not a feature that switches support.
NCR 6.2	Continuous monitoring	This requirement focuses on IPS/IDS functionality, not switches.
NCR 7.5	Emergency power	This test description focuses on security features in the switch's software not hardware functions.
NCR 7.6	Network security configuration settings	Suppliers rarely describe any guidelines on how to configure a switch.
NCR 7.8	Control system component inventory	Smaller LAN and industrial switches does not have the option to add additional components.

5 THE SCOPE OF THE PRODUCT TYPE TEST

The purpose of the product type test is to verify that the tested product has the properties that are required for a secure network. The result of this test will help the customers to choose the correct switch regarding to security requirement for their system.

6 PRODUCTION OF THE ITEM TO BE TESTED

Not applicable.

7 TEST EQUIPMENT

The switch (SW1), is the product that will be used for these test purposes.

7.1 Software configuration

The product referred to be tested should have the same firmware version as the corresponding IIT Certification previously performed. If it has not been or will be made an IIT Certification of the product the latest available firmware is to be used.

7.2 Hardware configuration

The following hardware configuration shall be used for the test:

- One computer (PC1) equipped with one Ethernet adapter and a serial port for system console connection. A serial to USB adapter may also be used instead of serial port. This PC is used to connect to the SWITCH using a terminal console or a web browser.
- Two clients (PC2 and PC3). Each equipped with one Ethernet adapter.
- Two servers (Server1 and Server2). Preferably running Ubuntu. It may be a physical servers or virtual servers.
- One switch (SW1). This switch is the main switch and also the one all tests are being made on.
- At least one extra switch (SW2). Some test requires the use of an extra switch.

Picture below shows complete topology of this test with all the required hardware that is needed and how it should be connected. The topology also shows recommended IP-addresses for each individual device. SW2 is not included in the topology but will be shown in a new topology when needed.

NOTE: PC1 does not need an IP-address if connected using console connection, however any available IP-address in the subnet range may be used when connecting to the GUI using a web browser.

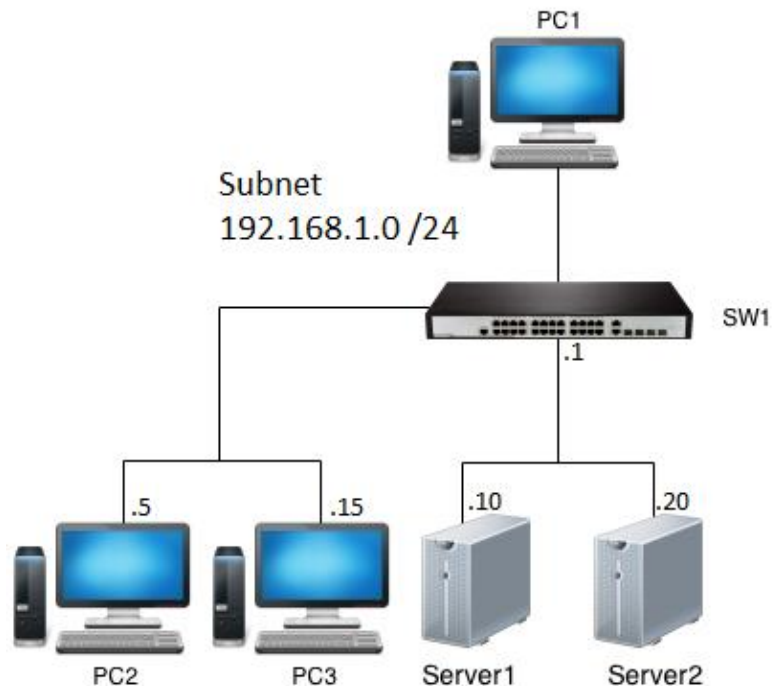


Figure 1: Hardware Configuration of full topology

7.3 Auxiliary Software for the test

Not applicable.

7.4 Tools

The following tools is recommended to be used for the test:

PUTTY (beta 0.63)	Application for terminal emulation and serial console connection.
TFTPD32 4.50 (Syslog server)	Application which includes various features such as Syslog server and TFTP server.
File Checksum Integrity Verifier	Application for computing and verifying cryptographic hash values for files.
VMware Player 6.0.2	Hypervisor application for creating and running virtual machines.
Ubuntu 13.10	Linux operating system
FreeRADIUS 3.0.3 (RADIUS server)	Application that offers RADIUS for authentication of users.
snmpd (SNMP client)	Tool used for sending SNMP GET Request.
ntpd (NTP server)	Application used to synchronize the time between network devices.
isc-dhcp-server (DHCP server)	A standardized networking protocol for dynamically distributing network configuration parameters.

7.5 Connection Method

Mount SW1 on a DIN rail or rack and equip it with power supply to boot it up. This process can take up to one to five minutes. Connect PC1 using any of the following methods.

- **Method 1:** Connect PC1 to the console port of SW1 and open a serial connection using a terminal such as PUTTY.
- **Method 2:** For switches using a graphical user interface (GUI) connect PC1 to any available port and follow the user manual of the switch for appropriate subnet for PC1 and connect to the specified default IP-address using a web browser of your choice.

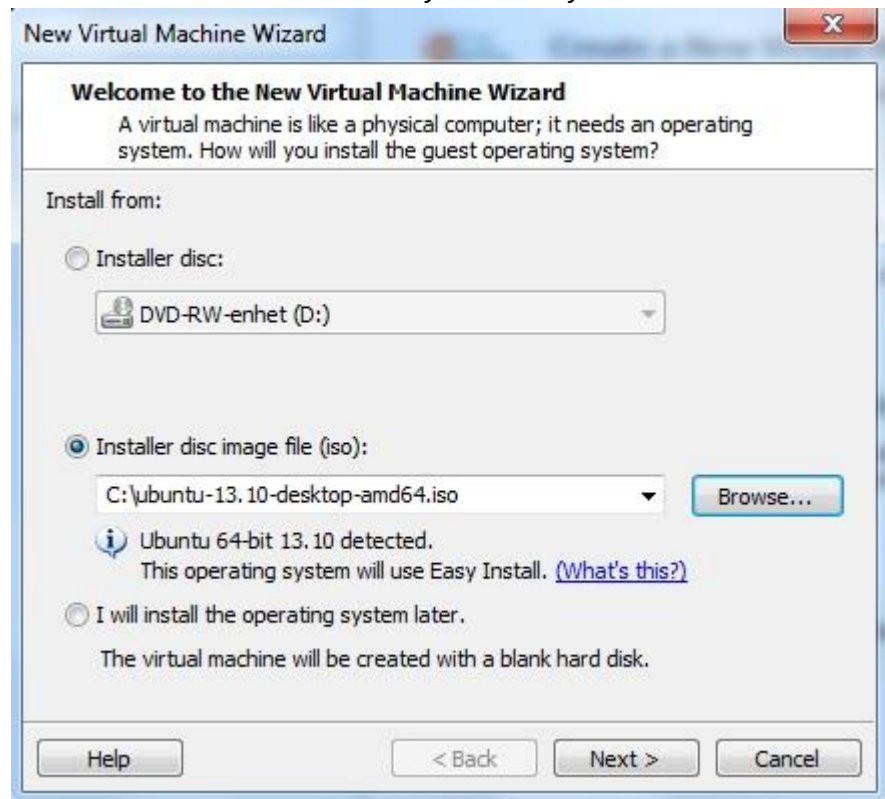


Figure 2: Hardware Configuration for switch test

7.6 Install Ubuntu 13.10 virtually

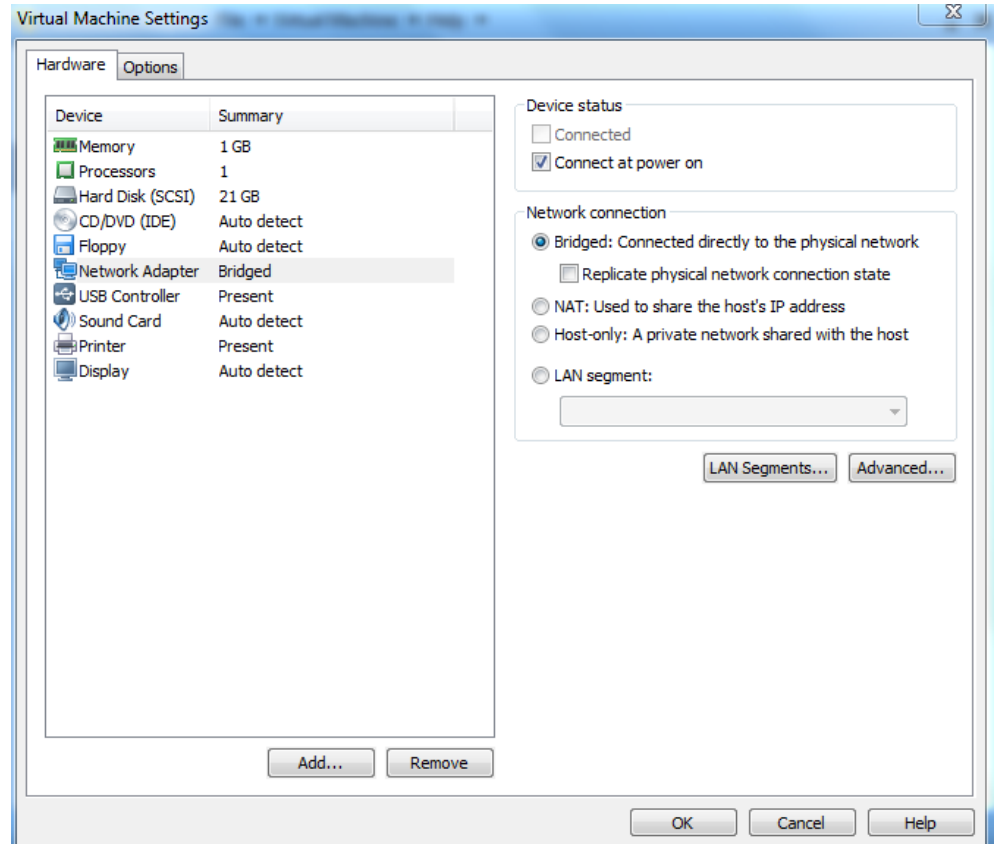
Ubuntu is a distribution of Linux that is easy to use and is well documented. To reduce costs and time Ubuntu can be installed virtually using VMware player. The steps below will guide you on how to install Ubuntu 13.10 using VMware Player 6.0.2 on Windows.

1. Make sure you have an internet connection, you need to have an internet connection through the whole installation.
2. Download and install VMware player.
 - a. Go to "http://www.wmware.com".
 - b. Download VMware player. This is a free product. If you have a license for VMware Workstation, it can be used instead.
 - c. When the program has been downloaded, install the program on the computer that you want your virtual Ubuntu computers to be located.
3. Download Ubuntu 13.10.
 - a. Go to http://www.ubuntu.com".
 - b. Download Ubuntu 13.10 for desktop use. This version might not be available at Ubuntu's website when you are trying to download it because the software is updated. Either you can use a search engine and download 13.10 from somewhere else, or download a later version of Ubuntu, but then we cannot guarantee that everything works as these guides suggests.
4. Install a new virtual computer.
 - a. Start VMware player and press "Create a new virtual machine".
 - b. Use the .iso-file for Ubuntu that you recently downloaded.

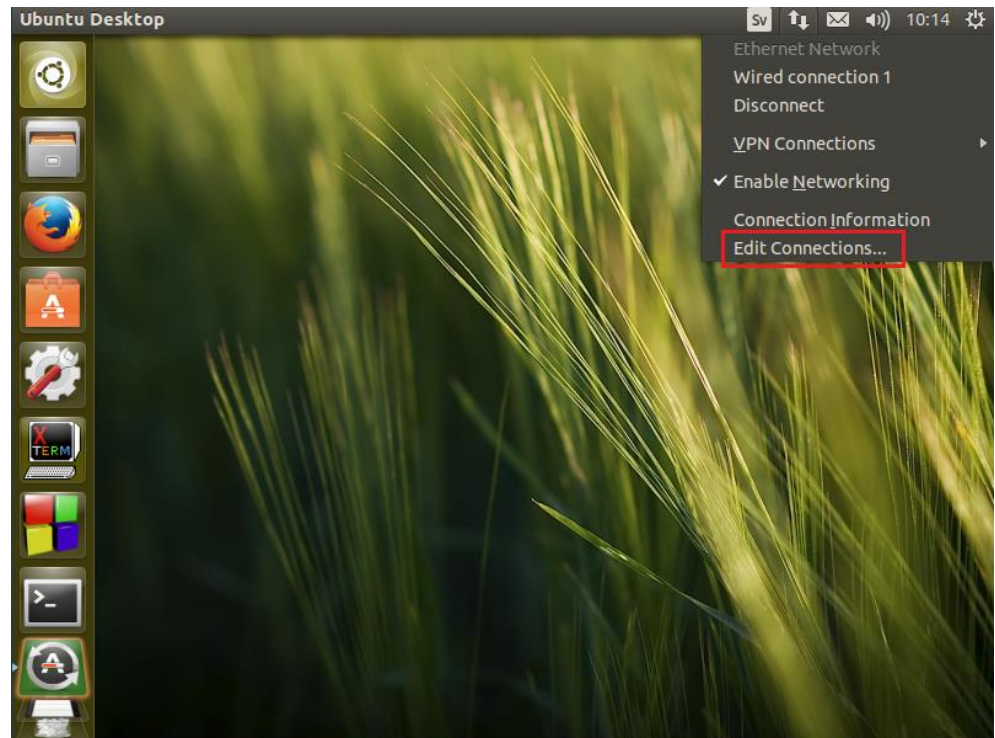


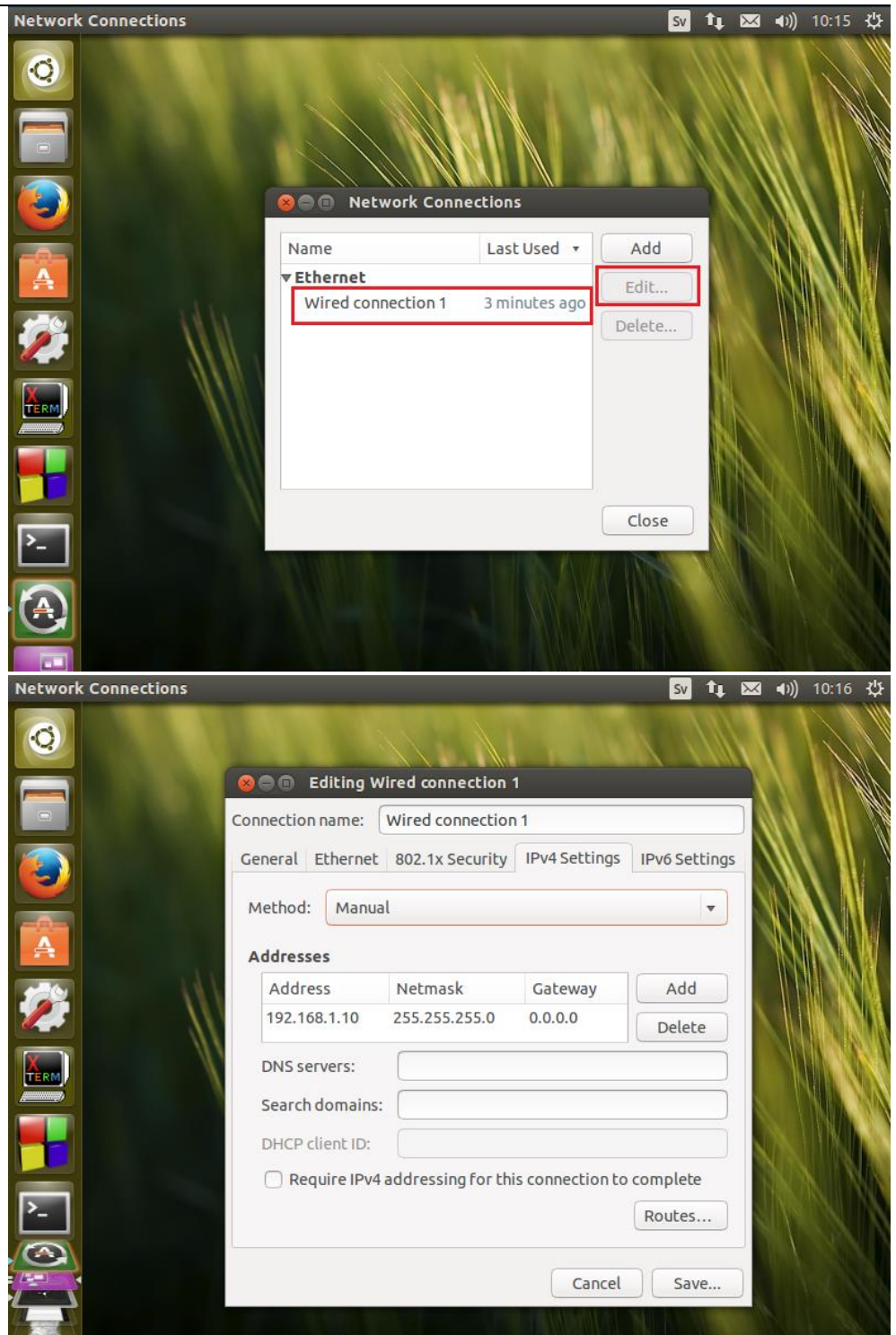
- c. Follow the guide until the computer is installed.
5. VMware Settings.
 - a. Go to settings in VMware player.

- b. Change the Network interface setting to be bridged instead of NAT. You do not have to “replicate physical network connection state”, it’s optional.



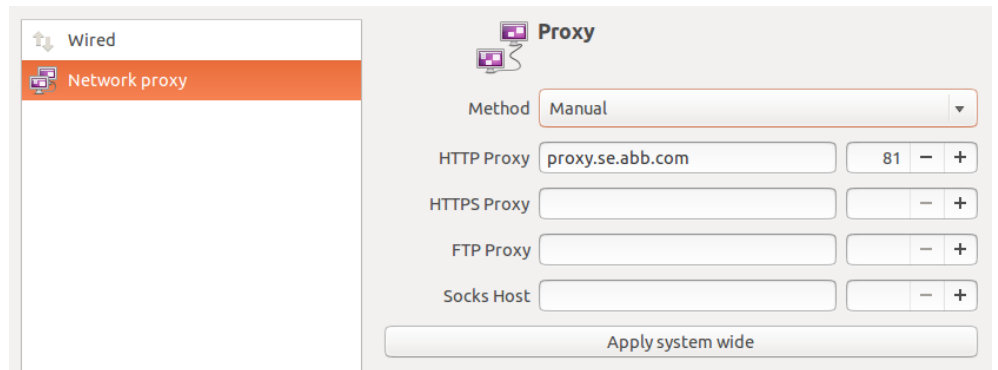
- c. Manually set an IP address that resides in the same subnet as your physical computer. Recommended is 192.168.1.10 for Server1 and 192.168.1.20 for Server2.



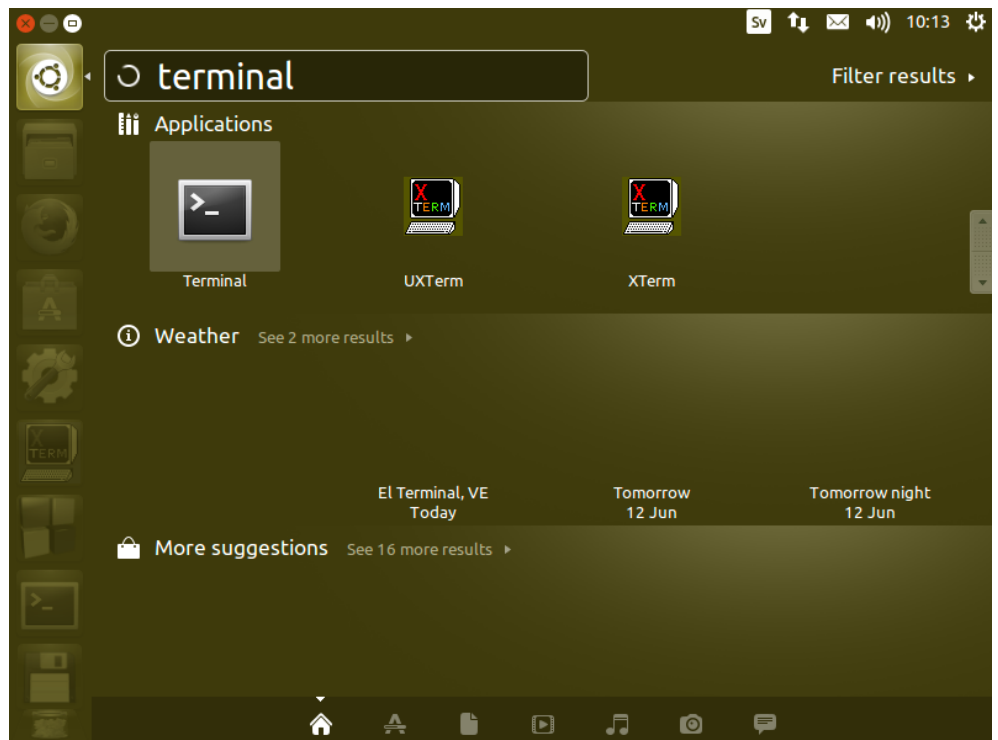


6. Configure the proxy settings (if needed).
 - a. Go to “System Settings” and then “Network”.

- b. Enter the DNS-name or IP-address of the proxy and the port number.



- c. Press “Apply system wide” and enter the password of your user account.
7. Update.
- a. Verify that you have internet connection.
- b. Start the terminal in Ubuntu.



- c. Write “`sudo apt-get update`” in terminal to update Ubuntu.
8. Repeat process from step 4 to install a second Ubuntu server which is needed for some redundancy tests later on.

8 TEST PROCEDURES

8.1 1 - Account Management

8.1.1 1.1 User accounts

8.1.1.1 The purpose of the test

This test will verify that the switch can add and remove user accounts in the switch's local database.

This test is based on these demands that the IEC62443-standard sets:

IEC 62443: NCR 1.1 Human user, process and device identification and authentication. States that the network component shall provide the capability to identify and authenticate all human users.

IEC 62443: NCR 1.3 Account management. States that the network component shall provide the capability to integrate into a system that supports the management of all accounts and/or provide the capability directly on the network device itself.

IEC 62443: NCR 1.5 Authenticator management. States that the network component shall be able to support the recognition of changes to default authenticators made at installation time.

8.1.1.2 Preparation and input data

Setup and connect the hardware according to the topology in Figure 1.

NOTE: If connected to the switch using GUI do not forget to have at least one additional account so you can log in using that if the test is successful. You do not want to lock yourself out from the switch.

8.1.1.3 Procedure

Part 1: Verify if it is possible to add additional user accounts.

1. Add a user account.
2. Logout from the switch and try to login using the new user account.

Part 2: Verify if it is possible to remove existing user accounts.

1. Remove a user from the local database.
2. Logout from the switch and try to login with the account that was recently removed.

Part 3: Verify if it is possible to change the password of an existing user account.

1. Change the password of an existing user account.
2. Logout from the switch and try to connect again using the old password, this should not work.
3. Try to login again using the correct password, this should work.

Part 4: Verify if it is possible to remove a preconfigured account.

1. Remove the preconfigured user from the local database.
2. Logout from the switch and try to login again with the account that was recently removed.

Part 5: Activate/disable a user account without removing it.

1. Log in to the switch using one of the user accounts configured on the switch local user-database.
2. Disable the account you just logged in with.
3. Disconnect from the switch and try to connect again with the account that was recently disabled.

8.1.1.4 Expected result

Part 1: The user will be able to login to the switch using the new account.

Part 2: The user will not be able to login to the switch using the deleted account.

Part 3: The user will be able to login to the switch using the new password.

Part 4: The user will not be able to login to the switch using the preconfigured account. If no pre-configured account exist the result is passed.

Part 5: The user will not be able to login to the switch using the disabled account.

8.1.2 1.2 Centralized authentication

8.1.2.1 The purpose of the test

This test will verify if the switch supports the ability to use centralized authentication.

This test is based on this demand that the IEC62443-standard sets:

IEC62443: NCR 1.3 Account management. States that the network component shall provide the capability to integrate into a system that supports the management of all accounts and/or provide the capability directly on the network device itself.

IEC62443: NCR 1.4 Identifier management. States that a network component that supports a direct user interface shall provide the capability to integrate into a system that supports the management of identifiers.

8.1.2.2 Preparation and input data

Configure the switch with an IP address if this has not already been done. VLAN 1 is normally the default management interface.

In this test you will need a RADIUS-server. An easy way to get a RADIUS-server is to install FreeRadius on a virtual Ubuntu machine. It is also possible to use a Windows Server that is using Active Directory.

These steps will guide you to install and setup FreeRadius on Ubuntu:

1. Verify that you have internet connection.
2. In terminal write “`sudo apt-get install freeradius`” and follow prompt.
3. Write command “`sudo gedit /etc/freeradius/clients.conf`” in the terminal. This will bring up a text file. In this file add the switch’s IP-address and password that is to be used to authenticate the RADIUS-server somewhere in this file, like this:

```
client 192.168.1.1 {
  secret = password-radius
}
```

 Save and close the text editor.
4. Write command “`sudo gedit /etc/freeradius/users`” in the terminal and add a user that you can use to log in to the switch with, like this:

```
testuser Cleartext-Password := "testpassword"
```

 Save and close the text editor.
5. Then write command “`sudo /etc/init.d/freeradius restart`”, for the changes to take effect. The RADIUS server is now up and running.

NOTE: The above commands is referring to a text-editor named “gedit”. Any other text editor could be used, alternatively navigating to the correct folder and file using the graphical user interface.

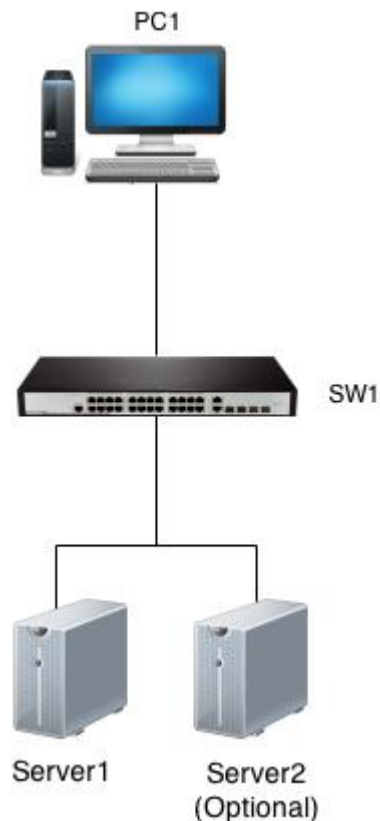


Figure 3: Hardware Configuration for RADIUS test

8.1.2.3 Procedure

Part 1: Verify that the authentication of connected users can be placed on a centralized server.

1. Setup the switch to use the RADIUS-server as its preferred method to authenticate users.
 - a. Add a RADIUS-server
 - i. Use the IP-address of the server that FreeRadius is installed on.
 - ii. The password is going to be "password-radius", if you are using this guide.
 - iii. If you are using FreeRadius the authentication-port is going to be 1812 and accounting-port is 1813
 - b. Create a method where the RADIUS-server is preferred method. You want to use the local-database as a backup if this does not work.
2. Login to the switch using an account that exist on the RADIUS-server, but not in the local user-database.
 - a. Open CLI program like PUTTY and try to Telnet or SSH to the device.
 - b. Login using username "testuser" and password "testpassword".

Part 2: Verify that the local user-database is used if the switch is unable to connect to the RADIUS-server.

1. When the RADIUS-server is still working: login to the switch using a user account that only exist on the RADIUS-server and not in the local user-database.
 - a. Connect with putty, or any other CLI program.
2. Disconnect the RADIUS-server.
 - a. Easiest way to do this is to shut down the interface in Ubuntu. This can be done either graphically or in the terminal by writing "`sudo ifconfig eth0 down`".
 - b. To enable the interface, write "`sudo ifconfig eth0 up`".
3. Try to login with the same user-account again.
 - a. Connect with putty, or any other CLI program.
 - b. This should now not work.
4. Login to the switch using an account that only exists in the local user-database.

Part 3: Verify if it is possible to use redundant RADIUS-servers.

1. Verify that you can add a second RADIUS-server, if not, the test ends here.
2. Install a second RADIUS-server.
 - a. Use the same steps as in "8.1.2.2".
3. Add the second RADIUS-server to the switch.
 - a. Create a group which contains both RADIUS-servers.
4. Disable the first RADIUS-server.
 - a. Easiest way to do this is to shut down the interface in Ubuntu. This can be done either graphically or in the terminal by writing "`sudo ifconfig eth0 down`".
 - b. To enable the interface, write "`sudo ifconfig eth0 up`".

5. Login to the switch using an account that does only exists on the RADIUS-servers.
 - a. This should work.
6. Re-enable the first RADIUS-server.
7. Disable the second RADIUS-server.
 - a. Easiest way to do this is to shut down the interface in Ubuntu. This can be done either graphically or in the terminal by writing "`sudo ifconfig eth0 down`".
 - b. To enable the interface, write "`sudo ifconfig eth0 up`".
8. Login to the switch using an account that does only exists on the RADIUS-servers.
 - a. This should work.

8.1.2.4 Expected result

Part 1: If you can login on the switch using a user account that only exists on the RADIUS-server, the test is successful.

Part 2: If you can login to the switch using an account that exists on the local user-database, the test is successful.

Part 3: If you can login to the switch at both step 5 and step 8, the test is successful.

8.1.3 1.3 Strength of password

8.1.3.1 The purpose of the test

This test will verify that the switch complies with these demands that the IEC62443-standard sets:

IEC 62443: NCR 1.7 Strength of password-based authentication. States that the network components that utilize password-based authentication, shall provide or integrate into a system that provides the capability to enforce:
Configurable password strength based on minimum length and variety of characters types and password minimum and maximum lifetime restrictions for human users. An enhancement to this requirement is to provide the capability to limit password reuse for a specific number of generations for human users.

8.1.3.2 Preparation and input data

No preparation needed.

8.1.3.3 Procedure

Configure the following password strength requirements for the switch management interface or a user:

- Configure password minimum length.
- Configure password complexity (e.g. upper-case, special-case characters).
- Configure password maximum lifetime restriction.
- Configure password minimum lifetime restriction.

Configure a new user or try to change the password or an existing user.

8.1.3.4 Expected result

When these configuration changes has been implemented they should be enforced immediately.

If lifetime restrictions cannot be set, the result is "Passed with remark". This is because lifetime restrictions is not really applicable on switches. This is because switches are not managed that often and it would be a burden to have to change the password every time the switch had to be managed.

8.1.4 1.4 User account privileges

8.1.4.1 The purpose of the test

The purpose of this test is to see if the switch is being able to customize roles with certain privileges for users. This solution of roles will make a scalable future.

This test is based on these demands that the IEC62443-standard sets:

IEC 62443-4-2: NCR 2.1 Authorization enforcement. States that if the network component supports a human user interface, it shall provide an authorization enforcement mechanism for all human users based on their assigned responsibilities.

8.1.4.2 Preparation and input data

At least two accounts should be available in the local user-database. You do not want to lock yourself out because of the restrictions you will set.

8.1.4.3 Procedure

Part 1: Change privileges on a user.

1. Configure a user account with other privileges than default.
 - a. It can be fixed settings, it could be set specifically based on the role or it could be just a preconfigured user with certain rights.
2. Verify that the changes has taken affect.
 - a. Log in to the switch using the account you changed the privileges on.

Part 2: Create a user with certain specific privileges.

1. Configure a user account with a set of specific privileges.
 - a. These privileges has to be manually set and not a pre-determined set of privileges that the switch already has configured.
2. Verify that the changes has taken affect.
 - a. Login to the switch using the account you changed the privileges on.

8.1.4.4 Expected result

Part 1: A user can be configured with a view other than default that restricts the use of that user account. This can also be a preconfigured guest user which only has read access or something similar.

Part 2: A user can be configured with a specific set of privileges that are manually set by the administrator.

8.2 2 - Sessions

8.2.1 2.1 Local sessions

8.2.1.1 The purpose of the test

The purpose is to test if a local session can get terminated both manually and automatically. This test is based on these demands that the IEC 62443 standard sets:

IEC 62443: NCR 1.1 Human user, process and device identification and authentication. The control system shall provide the capability to identify and authenticate all human users. This capability shall enforce such identification and authentication on all interfaces which provide human user access to the control system.

8.2.1.2 Preparation and input data

A computer with a terminal emulator such as PUTTY is needed to connect to the system console port.

8.2.1.3 Procedure

Verify that the session to the switch is terminated automatically after a certain time-period.

1. Set a maximum time-period which the user can be idle while connected to the console-port, if it is not set by default.
2. Wait till the command-line indicates that the user has been logged out.

8.2.1.4 Expected result

The user should be able to terminate the session manually, and automatically after a certain time-period.

8.2.2 2.2 Remote sessions

8.2.2.1 The purpose of the test

The purpose is to test if a remote session can get terminated both manually and automatically and by an admin. This test is based on these demands that the IEC 62443 standard sets:

IEC 62443: NCR 2.5 Session lock. The control system shall provide the capability to prevent further access by initiating a session lock after a configurable time period of inactivity. The session lock shall remain in effect until an authorized human unlocks the session.

IEC 62443: NCR 2.6 Remote session termination. States that the control system shall provide the capability to terminate a remote session either automatically after a configurable time period of inactivity or manually by the user who initiated the session.

8.2.2.2 Preparation and input data

No preparation needed.

8.2.2.3 Procedure

Part 1: Verify that the session is terminated automatically after a certain time-period.

1. Set a maximum time-period which the user can be idle while connected to the remote interface (CLI/GUI), if it is not set by default.
2. Wait till the command-line indicates that the user has been logged out.

Part 2: Verify that a user with privileges can terminate another user's session.

1. Connect to the switch using two different users.
2. Disconnect one of these users using the other user.

8.2.2.4 Expected result

The remotely connected user should be able to terminate the session manually and automatically after a certain time-period. The remotely connected user should also be able to get the connection terminated by an administrator.

8.2.3 2.3 SNMP

8.2.3.1 The purpose of the test

SNMP is an unsecure management protocol and should be disabled if not used. If used, the default community-strings should at least be changed.

This test is based on these demands that the IEC62443-standard sets:

IEC 62443: NCR 7.7 Least functionality. States that the control system shall provide the capability to specifically prohibit and/or restrict the use of unnecessary functions, ports, protocols and/or services.

8.2.3.2 Preparation and input data

This test requires SNMP to be installed on a computer to test SNMP-request against the switch.

These steps will guide you to install and setup SNMP on an Ubuntu machine. To simplify the SNMP-request, a MIBs packet is installed, which will make it possible to write the OID in a text-format, instead of a number-format.

1. In terminal write `sudo apt-get install snmp snmpd snmp-mibs-downloader` to install.
2. Write command `sudo gedit /etc/snmp/snmp.conf`. In this file comment out the row `"mibs :"`, with a `"#"` in front of the row. Like this `"# mibs :"`. Save and close the document.
3. Write command `sudo /etc/init.d/snmpd restart`, this will activate the changes just made.

8.2.3.3 Procedure

Part 1: Verify that SNMP can be disabled.

1. Disable SNMP.
2. Verify that a SNMP GetRequest does not get answered by the switch.
 - a. If you had to set the community-string, set it to “public” or change the community-string in the SNMP GetRequest to match the community-string set.
 - b. Use the following syntax to send a SNMP get request in the terminal in Ubuntu “snmpget -v 2c -c public 192.168.1.1 sysName.0”.

Part 2: Verify that the default SNMP community-strings can be changed.

1. Change the Read-only (RO) community-string for SNMP to something other than “public”.
2. Send a SNMP GetRequest to the switch using the default RO community-string “public”.
3. Verify that the GetRequest doesn’t get answered.
4. Send a SNMP GetRequest to the switch using the new community-string.
5. Verify that the request gets answered.

8.2.3.4 Expected result

Part 1: The switch doesn’t answer the SNMP GetRequest sent by the server.

Part 2: The switch doesn’t answer the SNMP GetRequest sent by the server using the default SNMP RO community-string after it has been changed.

8.2.4 2.4 SNMPv3

8.2.4.1 The purpose of the test

This test will verify if the switch is capable of using SNMP version 3. SNMP version 3 adds both authentication and encryption to the SNMP communication.

This test is based on these demands that the IEC62443-standard sets:

IEC 62443: NCR 4.1 Information confidentiality. States that the control system shall provide the capability to protect the confidentiality of information for which explicit read authorization is supported, whether at rest or in transit.

8.2.4.2 Preparation and input data

This test requires that SNMPv3 is installed on a computer. If you recently did test 2.3, you do not have to install anything, but if you didn't, use the guide in test 2.3.

These steps will guide you to setup SNMPv3 on an Ubuntu machine.

1. In terminal write "sudo gedit /etc/snmp/snmpd.conf".
2. In this file add the following line to add a username and password for SNMPv3
`createUser snmpuser MD5 snmppassword DES snmpencryption`
 Save and close the file.
3. The same user with the same passwords, authentication method and encryption method needs be created on the switch for this to work.

8.2.4.3 Procedure

1. Enable SNMPv3 on the switch.
 - a. SNMPv3 requires an authentication protocol, which is either MD5 or SHA1 and an encryption protocol, which is either DES, 3DES or AES. If these protocols can be changed; write down what protocols can be used for authentication and encryption on the switch.
2. Create a SNMPv3 user on the switch with the same username, passwords, authentication method and encryption method as in Ubuntu.
3. Verify that SNMPv3 GetRequests gets answered by the switch.
 - a. Use the following syntax to send a SNMPv3 GetRequest in Ubuntu
`terminal "snmpget -v 3 -u snmpuser -l authPriv -a MD5 -A snmppassword -x DES -X snmpencryption 192.168.1.1 sysName.0".`

8.2.4.4 Expected result

The Ubuntu server should be able to send a SNMPv3 GetRequest to the switch and get it answered.

If the authentication and encryption protocols can be changed; write down what protocols can be used for authentication and encryption on the switch.

8.2.5 2.5 Confine connections

8.2.5.1 The purpose of the test

This test shall verify that the switch can restrict management access from a certain IP subnet or IP address.

This test is based on these demands that the IEC62443-standard sets:

IEC 62443: NCR 1.13 Access via untrusted networks. States that the control system should restrict access achieved through dial-up connections (for example, limiting the dial-up access based upon the source of the request).

8.2.5.2 Preparation and input data

This test requires SNMP to be installed on a computer to send a SNMP GetRequest to the switch. This should already have been done in a previous step.

8.2.5.3 Procedure

Part 1: Verify that HTTP/HTTPS sessions can be confined to a certain IP subnet or IP address.

1. Verify that before any configuration, both of the clients can connect to the switch using the GUI.
 - a. If HTTPS is not enabled by default, proceed with just using HTTP.
2. Configure the switch to only accept the IP-address of one of the clients.
3. Try to connect to the switch using two different clients.
 - a. One of the clients should have an IP-address that is allowed to connect.
 - b. The other client should have an IP address that is not be allowed to connect.
4. Verify that only the allowed IP address is allowed to connect.

Part 2: Verify that Telnet/SSH sessions can be confined to a certain IP subnet or IP address.

1. Verify that before any configuration, both of the clients can connect to the switch using the CLI.
 - a. If SSH is not enabled by default, proceed with just using Telnet.
2. Configure the switch to only accept the IP address of one of the clients.
3. Try to connect to the switch using two different clients.
 - a. One of the clients should have an IP address that is allowed to connect.
 - b. The other client should have an IP address that is not be allowed to connect.
4. Verify that only the allowed IP-address is allowed to connect.

Part 3: Verify that SNMP sessions can be confined to a certain IP subnet or IP address.

1. Configure the switch to only accept SNMP-requests from the IP-address of the server with SNMP installed.
 - a. If you installed SNMP on both of your servers, you can allow one of them and disallow the other.
2. Verify that a SNMP-request using the allowed IP address is successful.
 - a. Use the following syntax in the terminal to send a SNMP GetRequest
`"snmpget -v 2c -c public 192.168.1.1 sysName.0"`
 - b. This should work.
3. Change the IP address of the server to something that should not be allowed.
4. Verify that a SNMP-request using an IP-address that is not allowed is denied.
5. Test the SNMP request again in step 2a.

8.2.5.4 Expected result

In each part the test is successful if it is possible to confine the connections to a certain IP subnet or IP address.

8.2.6 2.6 Limit concurrent connections**8.2.6.1 The purpose of the test**

This test shall verify that the switch can limit the number of concurrent connections. This test is based on these demands that the IEC62443-standard sets:

IEC 62443: NCR 2.7 Concurrent session control. States that the control system shall provide the capability to limit the number of concurrent sessions per interface for any given use to configurable number of sessions.

IEC 62443: NCR 7.2 Resource management. States that the control system shall provide the capability to limit the use of resources by security functions to prevent resource exhaustion.

8.2.6.2 Preparation and input data

No preparation needed.

8.2.6.3 Procedure

Part 1: Verify that the amount of concurrent Telnet/SSH-connections can be restricted.

1. Configure the switch to only accept one connection.
2. Try to connect to the switch using two CLIs.

Part 2: Verify that the amount of concurrent HTTP/HTTPS-connections can be restricted.

1. Configure the switch to only accept one connection.
2. Try to connect to the switch using two different windows/tabs in your internet browser.

8.2.6.4 Expected result

It should be possible to configure the number of open connections at a time. The test is passed with remark if the number of connections is fixed, but not configurable.

8.2.7 2.7 Secure connection methods

8.2.7.1 The purpose of the test

This test will verify that secure connection methods can be used for managing the switch. This is always a recommended best practices if the switch supports it. It will also test if the unsecure connection methods can be disabled.

This test is based on these demands that the IEC62443-standard sets:

IEC 62443: NCR 1.13 Access via untrusted networks. The control system shall provide the capability to monitor and control all methods of access to the control system via untrusted networks.

IEC 62443: NCR 3.1 Communication integrity. States that the network component shall provide the capability to protect the integrity of transmitted information. This should be provided as an internal functionality or through a compensating security mechanism.

IEC 62443: NCR 3.7 Session integrity. States that the network component shall provide the capability to protect the integrity of sessions.

IEC 62443: NCR 4.1 Information confidentiality. States that the control system shall provide the capability to protect the confidentiality of information for which explicit read authorization is supported, whether at rest or in transit.

IEC 62443: NCR 4.3 Use of cryptography. States that if cryptography is required, the network component shall use cryptographic security mechanisms according to internationally recognized and proven security practices and recommendations.

8.2.7.2 Preparation and input data

No preparation needed.

8.2.7.3 Procedure

Part 1: Verify that SSH can be used to configure the switch through the CLI.

1. Enable SSH on the switch.
 - a. SSH requires a RSA-key which is of a certain size and can sometimes be configured. Write down the size options in the test record.
2. Connect to the switch using SSH.

Part 2: Verify that HTTPS can be used to configure the switch through the GUI.

1. Enable HTTPS on the switch.
2. Connect to the switch using HTTPS from a web browser.

Part 3: Verify that Telnet-sessions to the switch can be disabled without disabling SSH.

1. Disable telnet on the switch.
2. Try connect using telnet. This should not work.

Part 4: Verify that HTTP-sessions to the switch can be disabled without disabling HTTPS.

1. Disable HTTP on the switch.
2. Try connect using HTTP. This should not work.

8.2.7.4 Expected result

- Part 1: SSH can be used instead of Telnet to connect to the switch.
Write down the size options for the RSA-key in the test record, if this can be found.
- Part 2: HTTPS can be used instead of HTTP to connect to the switch.
- Part 3: Telnet can be disabled without disabling SSH.
- Part 4: HTTP can be disabled without disabling HTTPS.

8.3 3 - Audit

8.3.1 3.1 Create audit-logs

8.3.1.1 The purpose of the test

This test shall verify that the switch can generate different level of logs both locally and on a centralized server. When sending the logs to a centralized server the format should be in an industry standard.

This test is based on these demands that the IEC62443-standard sets:

IEC 62443: NCR 2.11 Timestamps. States that the network component shall provide the capability to create timestamps (date and time) for use in audit records.

IEC 62443: NCR 2.8 Auditable events. States that the control system shall provide the capability to generate audit records relevant to security. Individual audit records shall include the timestamp, source, software process or human user account, category, type, event ID and event result.

IEC 62443: NCR 2.8 RE1 Auditable events - Centrally managed, system-wide audit trail. States that the control system shall provide the capability to centrally manage audit events. The control system shall provide the capability to export these audit records in industry standard formats for analysis by standard commercial log analysis tools.

IEC 62443: NCR 6.1 Audit log accessibility. States that the control system shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.

8.3.1.2 Preparation and input data

One of the requirements listed above states that the audit records should be in an industry standard. Syslog is an industry standard. Therefore this test requires that a syslog-server is installed on a server or computer.

A recommended program is TFTP32, it's a free program that you install on one of your computers with the Windows operating system.

8.3.1.3 Procedure

Part 1: Verify that the switch is capable to generate audit-logs locally.

1. Configure the switch to generate and save audit-logs locally.
2. Verify if the logs can be viewed on the switch.

Part 2: Verify that the switch is capable to generate audit-logs to a centralized server.

1. Configure the switch to send its audit-logs to the server.
2. Verify if the audit-logs can be viewed on the server.

Part 3: Verify that the level of information logged can be changed.

1. Change the level of information logged.
2. Verify if the change is implemented.

8.3.1.4 Expected result

Part 1: Logs should be able to be saved on the switch. The logs shall include timestamps, software process or human user account, category, type event ID and event result to reach passed result. For result "passed with remark" it shall just create a log with a description.

Part 2: Logs should be able to be saved on the switch. The logs shall include timestamps, software process or human user account, category, type event ID and event result to reach passed result. For result "passed with remark" it shall just create a log with a description.

Part 3: The level of information logged should be able to be changed.

8.4 4 - Login

8.4.1 4.1 Unsuccessful login attempts

8.4.1.1 The purpose of the test

This test will verify that unsuccessful login attempts will lock a user out from connecting to the switch.

This test is based on these demands that the IEC62443-standard sets:

IEC 62443-4-2: NCR 1.11 Unsuccessful login attempts. States that the network device shall provide the capability to enforce a limit of consecutive invalid access attempts by any user. The switch shall provide the capability to temporarily deny access when the maximum number of unsuccessful attempts is exceeded for a configurable time period or until the lockout is manually recovered.

8.4.1.2 Preparation and input data

Make sure that there are at least two user accounts in the local user-database. You do not want to be locked out if this test is successful.

Part 3 of this test requires that test 3.1 has been done and is successful.

8.4.1.3 Procedure

Part 1: Verify that a user can get locked when it has exceeded a number of unsuccessful login attempts within a certain time-period.

1. Configure the switch to lock a user if it unsuccessfully tries to login, if this is not done by default.
2. Try to login to the switch using telnet or SSH, purposefully using the wrong password.
 - a. Repeat a maximum of 10 times.
3. Verify that the user got locked by trying to login using the correct username and password.

Part 2: Verify that as an admin user you can unlock a locked user.

1. Use the other user account and try to unlock the locked user.
2. Verify that the user got unlocked by trying to login using the recently locked user.

Part 3: Verify that invalid access attempts to the switch are logged.

1. Configure the device to log invalid access attempts, if this is not by default.
2. Try to login to the switch, purposefully using the wrong password.
3. Verify on the syslog-server that a log as created about the invalid access attempt.

8.4.1.4 Expected result

Part 1: The user account will not be able to be used to login with.

Part 2: The user account will be able to be used to login with.

Part 3: A log event was created on the syslog-server.

8.4.2 4.2 System use notification

8.4.2.1 The purpose of the test

This test will verify that users that are trying to connect to the switch gets a message when accessing the device. This message could warn about consequences regarding a security breach of this device.

This test is based on these demands that the IEC62443-standard sets:

IEC 62443: NCR 1.12 System use notification. The control system shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel.

8.4.2.2 Preparation and input data

No preparation needed.

8.4.2.3 Procedure

1. Configure the switch to show a message at login.
2. Connect to the device using the CLI.
3. Connect to the device using the GUI.

8.4.2.4 Expected result

Part 1: A message is shown when before a user has entered its credentials, when using the CLI.

Part 2: A message is shown when before a user has entered its credentials, when using the GUI.

8.5 5 - Time

8.5.1 5.1 Change time

8.5.1.1 The purpose of the test

This test shall verify the ability to change time and date and to synchronize the time of the switch with a NTP-server. This test is based on these demands that the IEC 62443 standard sets:

IEC 62443-4-2: NCR 2.11 Timestamps. States that the network component shall provide the capability to create timestamps (date and time) for use in audit records.

8.5.1.2 Preparation and input data

In this test you will need a NTP-server. The easiest way to get a NTP-server is to install NTP on a virtual Ubuntu machine.

These steps will guide you to install and setup NTP on Ubuntu:

1. Install NTP by writing “`sudo apt-get install ntp`” in the terminal window and then follow the prompt.
2. Write command “`sudo gedit /etc/ntp.conf`” to open the ntp.conf file.
3. In this file add the following lines:
`server 127.127.1.0 iburst`
`fudge 127.127.1.0 stratum 10`
 Save and close the file.
4. Write command “`sudo /etc/init.d/ntp restart`”, for the changes to take effect.

The problem with this solution is that it cannot test NTP authentication. Which will make the next test not possible to carry out.

8.5.1.3 Procedure

Part 1: Verify that time and date can be changed manually.

1. Change the time on the switch
2. Verify that the time and date is correct.

Part 2: Verify that the switch can synchronize its time with a NTP-server.

1. Synchronize the time with the NTP-server.
2. Verify that the time and date is correct.

8.5.1.4 Expected result

Part 1: It should be possible to change the data and time on the switch manually.

Part 2: It should be possible to synchronize the time with a NTP-server.

8.5.2 5.2 Authentication

8.5.2.1 The purpose of the test

This test shall verify the increased security aspects of authentication with the NTP-server using passwords. This test is based on these demands that the IEC62443-standard sets:

IEC 62443: NCR 1.2 Software process and device identification and authentication. States that the network component shall provide the capability to identify itself and authenticate with any other component.

IEC 62443: NCR 2.11 RE2 Timestamps – Protection of time source integrity. States that the time synchronization mechanism shall provide the capability to detect unauthorized alteration.

8.5.2.2 Preparation and input data

For this test you cannot use the NTP-server that you installed in Ubuntu, because authentication is not implemented.

If the switch is a Cisco-switch you can configure another Cisco-switch or a Cisco-router to function as a NTP-server.

8.5.2.3 Procedure

Part 1: Verify that the switch can authenticate the NTP-server.

1. Synchronize the time with the NTP-server
2. Configure both the client and the server to use a password.
3. Verify that the time gets updated.

8.5.2.4 Expected result

The switch should be able to authenticate with the NTP-server.

8.6 6 - Port security general

8.6.1 6.1 Manual shutdown

8.6.1.1 The purpose of the test

This test shall verify that the switch can manually shut down ports. For example ports that are not being in use.

This test is based on this demand that the IEC62443-standard sets:

IEC 62443: NCR 7.7 Least functionality. States that the control system shall provide the capability to specifically prohibit and/or restrict the use of unnecessary functions, ports, protocols and/or services.

8.6.1.2 Preparation and input data

No preparation needed.

8.6.1.3 Procedure

1. Manually shut down a port.
2. Connect a client to that port and try to communicate with the switch.

8.6.1.4 Expected result

It should be possible to manually shut down a port on the switch and no traffic should flow on that specific port.

8.6.2 6.2 Rogue DHCP-server

8.6.2.1 The purpose of the test

The purpose of this test is to verify if the switch can protect the network against rogue DHCP-servers.

If an attacker connects a DHCP-server to a port of a switch this server could answer DHCP-requests from clients and by so changing the default-gateway which will redirect the traffic through one of the attacker's devices. This attack is a known man-in-the-middle attack and can be prevented successfully if the switch supports this feature.

This test is based on this demand that the IEC62443-standard sets:

IEC 62443: NCR 7.1 Denial of service protection. States that the control system shall provide the capability to manage communication loads (such as using rate limiting) to mitigate the effects of information flooding types of DoS events.

8.6.2.2 Preparation and input data

This test requires a DHCP-server. This could be an actual server working as a DHCP-server, but it can also be another switch or a router working as a DHCP-server.

These steps will guide you to install and setup DHCP server on Ubuntu:

1. In terminal write “`sudo apt-get install isc-dhcp-server`” to install the DHCP-server.
2. Write command “`sudo gedit /etc/default/isc-dhcp-server`”.
3. In this file we change the network interface card to be used if you have several. By default it listens to eth0. Remember this is optional and maybe not needed. By writing command “`ifconfig`” in the terminal you can figure out what NIC is used. Find this line “`INTERFACES=` ”. If eth1 is the NIC used; replace with the following line “`INTERFACES=eth1`”. Save the file and exit.
4. Write command “`sudo gedit /etc/dhcp/dhcpd.conf`”.
5. In this file we change the network configuration parameters. This is our example:
`default-lease-time 600;`
`max-lease-time 7200;`

```
subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.50 192.168.1.200;
  option subnet-mask 255.255.255.0;
  option broadcast-address 192.168.1.255;
  option routers 192.168.1.1;
  option domain-name-servers 192.168.1.1;
  option domain-name "yourdomainname.com";
}
```

Save and close the file.

6. Write command “`sudo /etc/init.d/isc-dhcp-server restart`”, for the changes to take effect.

NOTE: This will make the DHCP server distribute IP-addresses from the range 192.168.1.50-192.168.1.200 to clients. 192.168.1.1 will be used as default gateway.

8.6.2.3 Procedure

1. Activate DHCP-snooping.
2. Deny any DHCP-server-message from any port, this is normally the default action.
3. Connect a DHCP-server to one of these ports.
4. Request an IP-address using a client.
5. Verify that the port that is connect to the DHCP-server gets blocked.
6. Verify that the client never receives the IP-address.

8.6.2.4 Expected result

The client should not receive an IP-address from the DHCP-server.

8.6.3 6.3 DHCP rate limit

8.6.3.1 The purpose of the test

This test verifies if the switch can protect the network against a DHCP starvation attack. An attacker could use a program which randomizes its MAC-address and then requests an IP-address from the DHCP-server at a very fast rate. This will starve the DHCP-server from available IP-addresses and any legitimate client will not be able to retrieve an IP-address and therefore not be able to communicate with the rest of the network. This can be mitigated by setting a limit of how many DHCP-packets can be requested within one second.

This test is based on this demand that the IEC62443-standard sets:

IEC 62443: NCR 7.1 Denial of service protection. States that the control system shall provide the capability to manage communication loads (such as using rate limiting) to mitigate the effects of information flooding types of DoS events.

8.6.3.2 Preparation and input data

This test requires a DHCP-server. If you recently did test 6.2, this will already be done. Otherwise look at the "Preparation and input data" for test 6.2.

8.6.3.3 Procedure

1. Set a DHCP-request limit a port connected to a computer.
 - a. Set the rate to as low as possible so that any request will block the port.
2. Request an IP-address from the DHCP-server using the client.
3. Verify that the client's port gets blocked

8.6.3.4 Expected result

The switch should be able to block a port if too many DHCP-requests are being sent on that port.

8.7 7 - Port security against users

8.7.1 7.1 802.1x

8.7.1.1 The purpose of the test

The purpose of this test is to verify that the switch is able to authenticate users using 802.1x port-based authentication.

This test is based on this demand that the IEC62443-standard sets:

IEC 62443: NCR 1.1 Human user, process and device identification and authentication. States that the network component shall provide the capability to identify and authenticate all human users.

IEC62443: NCR 1.4 Identifier management. States that a network component that supports a direct user interface shall provide the capability to integrate into a system that supports the management of identifiers.

8.7.1.2 Preparation and input data

This test requires a computer with support for 802.1x authentication. It will probably also need a RADIUS-server up and running that should be used for authenticating users with, since the local user database on the switch is not enough sometimes.

Guide to activate 802.1x on a PC running Microsoft Windows 7:

1. Start run and write "services.msc", this should bring up the services window.
2. At the bottom of the window go to standard tab and search for "Wired AutoConfig".
3. Right click and start this service.
4. Next go to "Network Connections", right click on the correct NIC.
5. Choose properties and go to "authentication".
6. Check "Enable IEEE 802.1x authentication".
7. Go to "Settings" and then "Configure".
8. Uncheck the checkbox to automatically use the windows credentials.

8.7.1.3 Procedure

1. Configure 802.1x on the switch.
2. Verify that the client cannot communicate with the switch before the authentication-process.
3. Configure 802.1x support on the PC.
4. Authenticate to the switch using one of the user accounts on the RADIUS-server's database, or if it was possible, use the local database on the switch.
5. Verify that the client can communicate with the switch after the authentication-process.

8.7.1.4 Expected result

The client should be able to communicate with the switch after it has authenticated the user.

8.7.2 7.2 Port restrictions

8.7.2.1 The purpose of the test

This test will test the security functionality of port restrictions that can be made against users. These restrictions are useful because they can prevent users from adding their own switches/access-point to the network. Adding an unsecure switch/access-point to the network could open a hole in the network for anyone to connect that usually requires authentication.

A maximum number of users' restriction even mitigates an attack where the attacker tries to overflow the CAM-table of the switch in an attempt to eavesdrop on the traffic being sent.

This test is based on this demand that the IEC62443-standard sets:

IEC 62443: NCR 7.1 Denial of service protection. States that the control system shall provide the capability to manage communication loads (such as using rate limiting) to mitigate the effects of information flooding types of DoS events.

8.7.2.2 Preparation and input data

This test requires one additional switch. This switch can be any switch, even an unmanaged one. The test also requires two clients that will be used to send traffic to the switch.

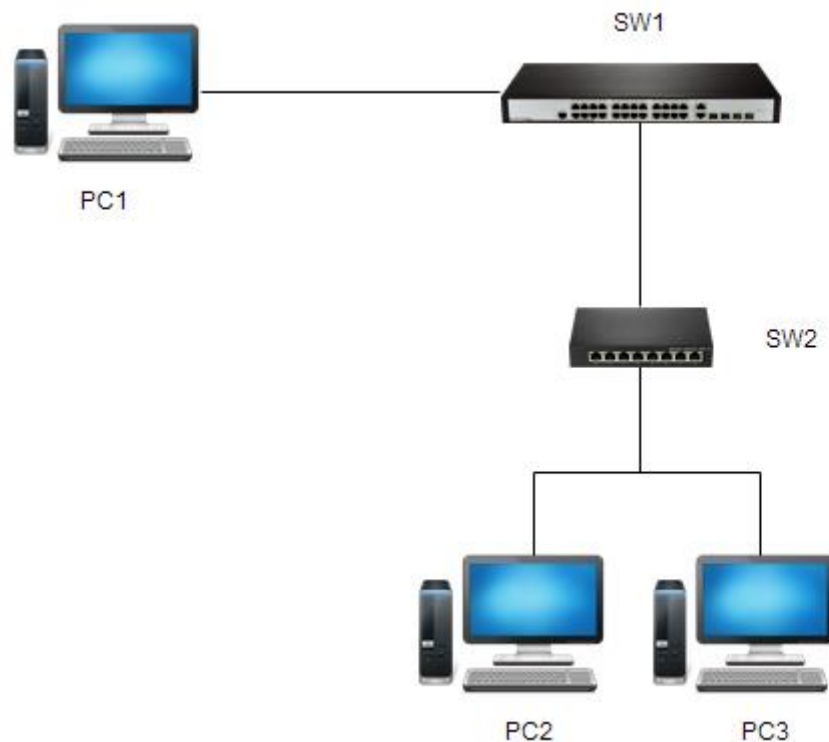


Figure 4: Hardware Configuration for port restrictions.

8.7.2.3 Procedure

Part 1: Verify that the amount of users can be restricted on a single port.

1. Configure a port to only accept traffic from one client.
2. Connect an additional switch to that port.
 - a. This switch can be a simple unmanaged switch.
3. Connect two clients to the new switch.
4. Send traffic to the switch using two clients connected to the second switch.
5. Verify that the port gets blocked.

Part 2: Verify that only certain MAC-addresses can connect to a certain port.

1. Configure a port to only accept one MAC-address.
2. Verify that the client can send traffic to the switch.
3. Connect another client to that port.
4. Verify that the new client cannot send traffic to the switch.

8.7.2.4 Expected result

Part 1: The switch should be able to restrict the number of users connected to a single port without restricting the port to a certain MAC address either by shutting down the port or by blocking the user violating the restrictions.

Part 2: The switch should be able to restrict a port to only accept traffic from certain MAC addresses either by shutting down the port or by blocking the user violating the restrictions.

8.8 8 - Other functionality

8.8.1 8.1 Network segmentation

8.8.1.1 The purpose of the test

This test will verify if the switch can logically segment the network by using Virtual Local Area Networks (VLANs). Segmentation of networks using VLANs is not for security reasons. The main reasons for segmenting networks are to reduce the spread, or egress, of network traffic from a control system.

This test is based on this demand that the IEC62443-standard sets:

IEC 62443: NCR 5.1 Network segmentation. States that the control system shall provide the capability to logically segment control system networks.

8.8.1.2 Preparation and input data

This test requires one switch and two clients that can use ping. Connect the two clients to any of the switches ports.

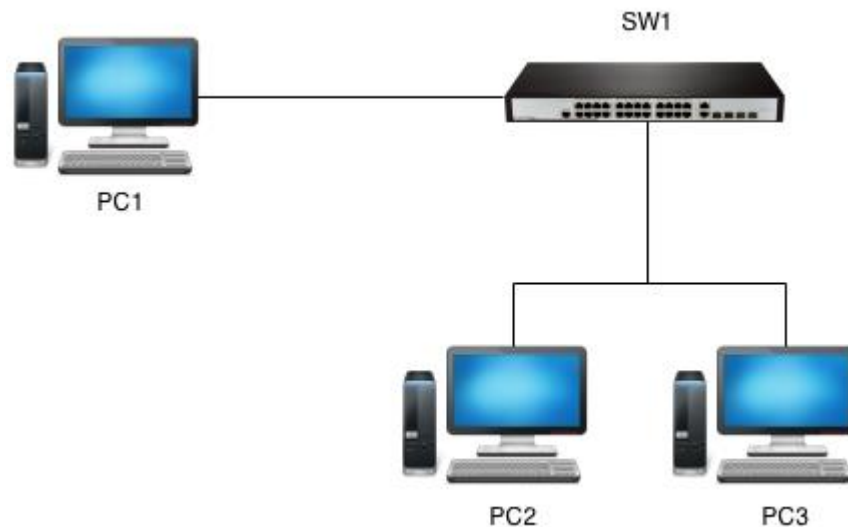


Figure 5: Hardware Configuration for other functionality

8.8.1.3 Procedure

1. Configure the switch with at least two VLANs.
2. Configure the ports that the clients are connected to, so they belong to the same VLAN.
3. Verify that the two clients can ping each other.
 - a. This should work
4. Configure one of the ports to belong to the other VLAN that was created in step 1.
5. Send a ping from the first machine to the second machine
 - a. This should now not work

8.8.1.4 Expected result

The two clients should not be able to ping each other when they belong to different VLANs.

8.8.2 8.2 Backup

8.8.2.1 The purpose of the test

This test will verify if the switch is capable to make a backup of the configuration-file on a client or server. It will also test if the backup can be automated.

This test is based on these demands that the IEC62443-standard sets:

IEC 62443: NCR 7.3 Control system backup. States that the control system shall support the ability to conduct backups of user-level and system-level information.

IEC 62443: NCR 7.3 RE2 Control system backup - Backup automation. States that the control system shall provide the capability to automate the backup function based on a configurable frequency.

IEC 62443: NCR 7.4 Control system recovery and reconstitution. States that the network component shall provide the capability to recover and reconstitute to a known secure state after a disruption or failure.

8.8.2.2 Preparation and input data

This test requires a TFTP server (or any similar file-transfer-protocol) to be running on one of the computers that will be used to send configuration backups to.

A recommended program is TFTP32, it's a free program that you install on one of your computers with the Windows operating system.

8.8.2.3 Procedure

Part 1: Verify that it is possible to make a backup of the configuration-file.

1. Use any file-transfer-protocol or other method to download the configuration-file from the switch to the computer.
2. Transfer the configuration-file to your computer.

Part 2: Verify that it is possible to automate the backup of the configuration-file.

1. Configure the switch to automate the backup-procedure.

Part 3: Verify that it is possible to load the configuration back on the switch and use it.

1. Save the configuration-file to your computer.
2. Make changes to the configuration-file.
3. Load the configuration-file to the switch and verify that all the changes made since the first saving has been undone.

8.8.2.4 Expected result

Part 1 & 2: The configuration-file should appear in the folder that was specified in the download. The backup does not have to be saved remotely, it can also be saved locally on the switch.

Part 3: The switch can load in an old version of the configuration-file and use it.

8.8.3 8.3 Spanning-tree – block BPDUs

8.8.3.1 The purpose of the test

This test will verify that the switch can block BPDUs that are received from a port where a switch should not exist.

When a switch is connected on another port than it should it could be an attacker who is trying to access the network by attaching its own switch. Blocking this port when this occurs successfully mitigates this risk and it will notify the administrator that a switch has been attached to the network by a user.

8.8.3.2 Preparation and input data

This test needs two switches. Both of these switches have to use spanning-tree.

8.8.3.3 Procedure

1. Configure one of the switch's port to block BPDUs.
2. Connect the other switch to that port.
3. Verify that the switch doesn't recognize the other switch as a valid spanning-tree neighbor by blocking the port or something similar.

8.8.3.4 Expected result

The switch will either ignore the BPDUs received on the port or shut down the port.

8.8.4 8.4 Spanning-tree – protect the root switch

8.8.4.1 The purpose of the test

This test will verify if the switch can protect the spanning-tree topology from BPDUs that contains lower priority than should appear on a port.

In a spanning-tree topology it is the switch with the lowest BPDU-priority that possesses the role of the root. If an attacker possesses the role of the root, all traffic will go through the attacker's switch and the attacker will be able to listen for passwords etc, or even carry out a man-in-the-middle attack.

8.8.4.2 Preparation and input data

This test needs two switches. Both of these switches have to use spanning-tree.



Figure 6: Hardware configuration for spanning-tree.

8.8.4.3 Procedure

1. Configure spanning-tree on SW1 with the second lowest priority possible for a VLAN.
 - a. This will probably be 4096, if nothing else is specified in the CLI/GUI.
2. Configure SW1 to guard the root switch on the port which you will connect SW2 on.
3. Configure spanning-tree on SW2 with the lowest priority than SW1.
 - a. This will probably be 0, if nothing else is specified in the CLI/GUI.
4. Connect SW2 to the port of SW1 that was configured to protect the root.

8.8.4.4 Expected result

The port should be disabled or shut down to prevent the other switch from becoming the root of the spanning-tree topology.

8.9 9 - Confidentiality

8.9.1 9.1 Encrypt passwords

8.9.1.1 The purpose of the test

This test will verify if the passwords in the configuration-file can be encrypted.

This test is based on this demand that the IEC62443-standard sets:

IEC 62443: NCR 1.14 Strength of symmetric key authentication shall provide the capability to store the shared secret securely.

8.9.1.2 Preparation and input data

Verify that there are unencrypted passwords in the configuration-file.

8.9.1.3 Procedure

Configure the switch to encrypt all username passwords in the configuration-file.

8.9.1.4 Expected result

Passwords in the configuration-file is encrypted.

If the passwords are already encrypted or hidden without any configuration, the result is "Passed". If there is no way to get hold of the configuration-file, like on a simple GUI-managed switch, the result is "Not applicable".

8.9.2 9.2 Integrity check

8.9.2.1 The purpose of the test

This test will verify that the switch is able to create a MD5 or an SHA1 checksum of files in its memory. This MD5/SHA1 checksum can be used to verify the integrity of a file. This is a good practice before installing a new firmware, because it will verify that the firmware isn't damaged.

This test is based on this demands that the IEC62443-standard sets:

IEC 62443: NCR 3.4 Software and information integrity. States that network components shall provide the capability to perform or support integrity checks on software, configuration and other information as well as recording and reporting the results of these checks.

8.9.2.2 Preparation and input data

Download and install a program that can compute a MD5 or SHA1 checksum on your computer, e.g. "Microsoft File Checksum Integrity Verifier".

Usage guide on Microsoft File Checksum Integrity Verifier.

1. Use a search engine and search for "Microsoft File Checksum Integrity Verifier".
2. Download the program.
3. Install the program, preferably in your home-folder, because you will have to navigate through the cmd to this folder.
4. Press start-button in windows and search for "cmd".
5. Navigate yourself to the folder you installed the program by using "cd /FOLDERNAME" to enter a folder, or "cd .." to go backwards.
6. Write "fciv.exe -add c:<folder-path-to-file-to-compute-checksum>"
 - a. If the configuration-file or firmware is in the same folder as fciv.exe, you just have to enter the name of the file.
7. Copy the computed checksum into notepad and save.

8.9.2.3 Procedure

Part 1: Create a MD5/SHA1 checksum of the configuration-file.

1. Transfer a copy of the configuration-file to a computer.
 - a. For this you can use TFTP or any other protocol available.
2. Create the checksum on the computer of the configuration file.
3. Create the checksum on the switch of the configuration-file.

Part 2: Create a MD5/SHA1 checksum of the firmware.

1. Transfer a copy of the firmware to a computer.
 - a. For this you can use TFTP or any other protocol available.
2. Create the checksum on the computer of the configuration file.
3. Create the checksum on the switch of the configuration-file.

8.9.2.4 Expected result

The test is success if it is possible to compute a checksum of the configuration-file/firmware on the switch and if the computed checksum from the switch and the computed checksum from the software on the computer is the same.

9 APPENDICES

Not applicable.

Security Feature-test for Ethernet Switches

Product Type Test Record

Cisco IE 3000-8TC

Type des.		Part no.					
Prep.	/ Henrik Grankvist	2014-06-17	Doc. kind	Type Test Record Security Feature-test for Ethernet Switches	No. of p. 21		
Appr.	/						
Resp. dept	Draft						
 ABB AB			Doc. no.	3BSE080141	Lang. en	Rev. ind.	Page 1

1.	TEST RESULT OVERVIEW	3
2.	TYPE TEST RESULT – VERSION 1	5
2.1	General	5
2.1.1	Test performed by	5
2.1.2	Vendor and product information	5
2.2	Test Equipment	6
2.2.1	Software	6
2.2.2	Hardware	6
2.2.3	Test application	6
2.2.4	Automatic test	6
2.2.5	Tools	6
2.3	Test Result	7
2.3.1	1 - Account management	7
2.3.1.1	1.1 User accounts	7
2.3.1.2	1.2 Centralized authentication	8
2.3.1.3	1.3 Strength of password	9
2.3.1.4	1.4 User account privileges	9
2.3.2	2 - Sessions	10
2.3.2.1	2.1 Local sessions	10
2.3.2.2	2.2 Remote sessions	10
2.3.2.3	2.3 SNMP	11
2.3.2.4	2.4 SNMPv3	11
2.3.2.5	2.5 Confine connections	11
2.3.2.6	2.6 Limit concurrent connections	12
2.3.2.7	2.7 Secure connection methods	13
2.3.3	3 - Audit	14
2.3.3.1	3.1 Create audit-logs	14
2.3.4	4 - Login	15
2.3.4.1	4.1 Unsuccessful login attempts	15
2.3.4.2	4.2 System use notification	16
2.3.5	5 - Time	16
2.3.5.1	5.1 Change time	16
2.3.5.2	5.2 Authentication	17
2.3.6	6 - Port security general	17
2.3.6.1	6.1 Manual shutdown	17
2.3.6.2	6.2 Rogue DHCP-server	17
2.3.6.3	6.3 DHCP-rate-limit	17
2.3.7	7 - Port security against users	18
2.3.7.1	7.1 802.1x	18
2.3.7.2	7.2 Port restrictions	18
2.3.8	8 - Other functionality	19
2.3.8.1	8.1 Network segmentation	19
2.3.8.2	8.2 Backup	19
2.3.8.3	8.3 Spanning-tree – block BPDUs	19
2.3.8.4	8.4 Spanning-tree – protect the root switch	20
2.3.9	9 - Confidentiality	20
2.3.9.1	9.1 Encrypt passwords	20
2.3.9.2	9.2 Integrity check	20
2.4	Remark list	21
2.5	Conclusions of the test	21

1. TEST RESULT OVERVIEW

Test no.	Test Case description	Result
1.1.1	Add user account	Passed
1.1.2	Remove user account	Passed
1.1.3	Remove preconfigured user account	Passed
1.1.4	Activate/Disable user account without removing it	Failed
1.2.1	Handle authentication on centralized server	Passed
1.2.2	Local database as backup if centralized authentication-server fails	Passed
1.2.3	Redundant centralized authentication-servers	Passed
1.3	Force a certain strength on new passwords	Passed
1.4.1	User accounts with different privileges	Passed
1.4.2	Create custom made privileges	Passed
2.1	Automatically terminate local sessions after a configurable time-period	Passed
2.2.1	Automatically terminate remote sessions after a configurable time-period	Passed
2.2.2	Terminate another users connection	Passed
2.3.1	Disable SNMP	Passed
2.3.2	Change default SNMP community-string	Passed
2.4	SNMPv3	Passed
2.5.1	Confine HTTP/HTTPS connections to a certain IP-address/subnet	Passed
2.5.2	Confine Telnet/SSH connections to a certain IP-address/subnet	Passed
2.5.3	Confine SNMP-requests to a certain IP-address/subnet	Passed
2.6.1	Limit concurrent Telnet/SSH connections	Passed
2.6.2	Limit concurrent HTTP/HTTPS connections	Failed with remark
2.7.1	Enable SSH	Passed
2.7.2	Enable HTTPS	Passed
2.7.3	Disable Telnet	Passed
2.7.4	Disable HTTP	Passed
3.1.1	Create and save audit-logs on local switch	Passed
3.1.2	Create and send audit-logs to centralized server	Passed
3.1.3	Change level of information logged	Passed
4.1.1	Lock a user after a number of unsuccessful login attempts	Passed
4.1.2	Unlock locked user	Passed
4.1.3	Create log event on unsuccessful login attempts	Passed
4.2.1	System use notification CLI	Passed
4.2.2	System use notification GUI	Failed
5.1.1	Change the time manually	Passed
5.1.2	Change the time using NTP	Passed
5.2	Authenticate the NTP-server	Passed

Test no.	Test Case description	Result
6.1	Manually shut down a port	Passed
6.2	Protect against rogue DHCP-servers	Failed with remark
6.3	Implement DHCP-rate-limit	Failed with remark
7.1	802.1x	Passed
7.2.1	Set a maximum number of users that can communicate on a single port	Passed
7.2.2	Set what MAC-addresses can communicate on a single port	Passed
8.1	Logically segment the network using VLANs	Passed
8.2.1	Manually backup the configuration-file	Passed
8.2.2	Automated backup of configuration file.	Passed
8.3	Block BPDUs on access-ports	Passed
8.4	Protect the root switch in a spanning-tree topology	Passed
9.1	Encrypt passwords in the configuration-file	Passed
9.2.1	Compute MD5/SHA1 checksum on configuration-file	Passed
9.2.2	Compute MD5/SHA1 checksum on firmware	Passed

2. TYPE TEST RESULT – VERSION 1

2.1 General

2.1.1 Test performed by

Test Description, id, title and version			
☒ Formal test		☐ Informal test	
Tested by (name):		Initials:	
Henrik Grankvist		HG	
Test started (date):	20-05-2014	Test ended (date):	21-05-2014
Total Time Spent (man hours):	0		8

Test Description, id, title and version			
☒ Formal test		☐ Informal test	
Tested by (name):		Initials:	
William Kvarnström		WK	
Test started (date):	20-05-2014	Test ended (date):	21-05-2014
Total Time Spent (man hours):	0		8

2.1.2 Vendor and product information

Vendor	Cisco
Product	IE-3000-8TC
Hardware version	
Software version	IES-IPSSERVICESH9-M version 15.0(2)SE5

2.2 Test Equipment

2.2.1 Software

The product referred to be tested should have the same firmware version as the corresponding IIT Certification previously performed. If it has not been or will be made an IIT Certification of the product the latest available firmware is to be used.

2.2.2 Hardware

The following hardware configuration shall be used for the test:

- One computer (PC1) equipped with one Ethernet adapter and a serial port for system console connection. A serial to USB adapter may also be used instead of serial port. This PC is used to connect to the SWITCH using a terminal console or a web browser.
- Two clients (PC2 and PC3). Each equipped with one Ethernet adapter.
- Two servers (Server1 and Server2). Preferably running Ubuntu. It may be a physical servers or virtual servers.
- One switch (SW1). This switch is the main switch and also the one all tests are being made on.
- At least one extra switch (SW2). Some test requires the use of an extra switch.

2.2.3 Test application

Not applicable.

2.2.4 Automatic test

Not applicable.

2.2.5 Tools

The following tools is recommended to be used for the test:

PUTTY (beta 0.63)	Application for terminal emulation and serial console connection.
TFTPD32 4.50 (Syslog server)	Application which includes various features such as Syslog server and TFTP server.
File Checksum Integrity Verifier	Application for computing and verifying cryptographic hash values for files.
VMware Player 6.0.2	Hypervisor application for creating and running virtual machines.
Ubuntu 13.10	Linux operating system
FreeRADIUS 3.0.3 (RADIUS server)	Application that offers RADIUS for authentication of users.
snmpd (SNMP client)	Tool used for sending SNMP GET Request.
ntpd (NTP server)	Application used to synchronize the time between network devices.
isc-dhcp-server (DHCP server)	A standardized networking protocol for dynamically distributing network configuration parameters.

2.3 Test Result

Result

The results that should be used are: Passed, Passed with remarks, Failed, Failed with remark, Not applicable or Not tested. Not applicable is for example the result when there is a test about the CLI but the switch doesn't have the CLI as a connection method. If there is a result that doesn't fit any of these results, write an explanation.

Remark ID

If the test is passed but there are unexpected results, write a remark. Also if the switch states somehow that it supports a certain feature but the test disclaims that support, write a remark.

Date

Write the date that the test was taken.

Signature

Write the signature of the person who carried out the test. The signature here should match the signature written under "Test performed by".

Procedure

Write down the steps taken to complete the test. For example; the commands written in the CLI or tabs pressed in the GUI.

2.3.1 1 - Account management

2.3.1.1 1.1 User accounts

Part 1 – Add user account

Result:	Remark ID	Date	Signature
Passed		20-05-2014	HG / WK

Procedure

```
switch(config)# username admin password admin123
```

Part 2 – Remove user account

Result:	Remark ID	Date	Signature
Passed		20-05-2014	HG / WK

Procedure

```
switch(config)# no username admin
```

Part 3 – Remove preconfigured user account

Result:	Remark ID	Date	Signature
Passed		20-05-2014	HG / WK

Procedure

No preconfigured accounts exist.

Part 4 – Activate/Disable user account without removing it

Result:	Remark ID	Date	Signature
Failed		20-05-2014	HG / WK

Procedure

2.3.1.2

1.2 Centralized authentication

Part 1 - Handle authentication on centralized server

Result:	Remark ID	Date	Signature
Passed		20-05-2014	HG / WK

Procedure

```
switch(config)# aaa new-model
switch(config)# aaa group server radius RADIUS-GROUP
switch(config-sg-radius)# server-private 192.168.1.10 auth-port
1812 acct-port 1813 key password-radius
switch(config)# aaa authentication login default group RADIUS-GROUP
```

Part 2 - Local database as backup if centralized authentication-server fails

Result:	Remark ID	Date	Signature
Passed		20-05-2014	HG / WK

Procedure

```
switch(config)# aaa authentication login default group RADIUS-GROUP
local-case
```

Part 3 - Redundant centralized authentication-servers

Result:	Remark ID	Date	Signature
Passed		20-05-2014	HG / WK

Procedure

```
switch(config-sg-radius)# server-private 192.168.1.20 auth-port
1812 acct-port 1813 key password-radius
```

2.3.1.3

1.3 Strength of password

Force a certain strength of new passwords

Result:	Remark ID	Date	Signature
Passed with remark	1	20-05-2014	HG / WK

Procedure

```
switch(config)# aaa new-model
switch(config)# aaa authentication default local-case
switch(config)# aaa common-criteria policy POLICY1
switch(config-co-policy)# min-length 5
switch(config-co-policy)# upper-case 1
switch(config-co-policy)# min-length 1
switch(config-co-policy)# special-case 1
switch(config-co-policy)# lifetime day 30
```

2.3.1.4

1.4 User account privileges

Part 1 - User accounts with different privileges

Result:	Remark ID	Date	Signature
Passed		20-05-2014	HG / WK

Procedure

```
switch(config)# aaa new-model
switch(config)# aaa authentication login default local
switch(config)# aaa authentication exec default local
switch(config)# username support privilege-level 3 password testpw
```

Part 2 - Create custom made privileges

Result:	Remark ID	Date	Signature
Passed		20-05-2014	HG / WK

Procedure

```
switch(config)# privilege exec level 3 show startup-config
```

2.3.2 2 - Sessions

2.3.2.1 2.1 Local sessions

Automatically terminate local sessions after a configurable time-period

Result:	Remark ID	Date	Signature
Passed		20-05-2014	HG / WK

Procedure

```
switch(config)# line console 0
switch(config-line)# exec-timeout 1
```

2.3.2.2 2.2 Remote sessions

Part 1 - Automatically terminate remote sessions after a configurable time-period

Result:	Remark ID	Date	Signature
Passed		20-05-2014	HG / WK

Procedure

```
switch(config)# line vty 0 15
switch(config)# exec-timeout 1
```

Part 2 - Terminate another user's connection

Result:	Remark ID	Date	Signature
Passed		20-05-2014	HG / WK

Procedure

```
switch# clear line vty 0
```

2.3.2.3

2.3 SNMP

Part 1 - Disable SNMP

Result:	Remark ID	Date	Signature
Passed		20-05-2014	HG / WK

Procedure

```
Disabled by default.
switch(config)# no snmp-server
```

Part 2 - Change default SNMP community-string

Result:	Remark ID	Date	Signature
Passed		20-05-2014	HG / WK

Procedure

```
switch(config)# snmp-server community ro new-read-only-password
switch(config)# snmp-server community rw new-read-write-password
```

2.3.2.4

2.4 SNMPv3

Implement SNMPv3

Result:	Remark ID	Date	Signature
Passed		20-05-2014	HG / WK

Procedure

```
switch(config)# snmp-server group SNMP-GROUP v3 priv
switch(config)# snmp-server smpuser SNMP-GROUP v3 auth md5
snmppassword priv des snmpencryption
```

2.3.2.5

2.5 Confine connections

Part 1 - Confine HTTP/HTTPS connections to a certain IP-address/subnet

Result:	Remark ID	Date	Signature
Passed		20-05-2014	HG / WK

Procedure

```
switch(config)# ip access-list standard 1
switch(config-std-nal)# permit host 192.168.1.5
switch(config)# ip http access-class 1
```

Part 2 - Confine Telnet/SSH connections to a certain IP-address/subnet

Result:	Remark ID	Date	Signature
Passed		20-05-2014	HG / WK

Procedure

```
switch(config)# ip access-list standard 1
switch(config-std-nacl)# permit host 192.168.1.5
switch(config)# line vty 0 15
switch(config)# access-class 1 in
```

Part 3 - Confine SNMP-requests to a certain IP-address/subnet

Result:	Remark ID	Date	Signature
Passed		20-05-2014	HG / WK

Procedure

```
switch(config)# switch(config)# ip access-list standard 1
switch(config-std-nacl)# permit host 192.168.1.10
switch(config)# snmp-server community ro public 1
```

2.3.2.6

2.6 Limit concurrent connections

Part 1 - Limit concurrent Telnet/SSH connections

Result:	Remark ID	Date	Signature
Passed		20-05-2014	HG / WK

Procedure

```
switch(config)# ip access-list standard 1
switch(config-std-nacl)# deny any
switch(config)# line vty 1 15
switch(config-line)# access-class 1 in
or
switch(config)# line vty 1 15
switch(config-line)# transport input none
```

Part 2 - Limit concurrent HTTP/HTTPS connections

Result:	Remark ID	Date	Signature
Failed with remark		20-05-2014	HG / WK

Procedure

2.3.2.7 2.7 Secure connection methods

Part 1 - Enable SSH

Result:	Remark ID	Date	Signature
Passed		20-05-2014	HG / WK

Procedure

```
switch(config)# crypto key generate rsa 1024 modulus general-keys
switch(config)# ip ssh version 2
```

Part 2 - Enable HTTPS

Result:	Remark ID	Date	Signature
Passed	2	20-05-2014	HG / WK

Procedure

```
Enabled by default.
switch(config)# ip http secure-server
```

Part 3 - Disable Telnet

Result:	Remark ID	Date	Signature
Passed		20-05-2014	HG / WK

Procedure

```
switch(config)# line vty 0 15
switch(config)# transport input ssh
```

Part 4 - Disable HTTP

Result:	Remark ID	Date	Signature
Passed		20-05-2014	HG / WK

Procedure

```
switch(config)# no ip http server
```

2.3.3 3 - Audit

2.3.3.1 3.1 Create audit-logs

Part 1 - Create and save audit-logs on local switch

Result:	Remark ID	Date	Signature
Passed		20-05-2014	HG / WK

Procedure

```
switch(config)# logging buffered
switch# show logging
```

Part 2 - Create and send audit-logs to centralized server

Result:	Remark ID	Date	Signature
Passed		20-05-2014	HG / WK

Procedure

```
switch(config)# logging host 192.168.1.10
```

Part 3 - Change level of information logged

Result:	Remark ID	Date	Signature
Passed		20-05-2014	HG / WK

Procedure

```
switch(config)# logging trap 3
```

2.3.4 4 - Login

2.3.4.1 4.1 Unsuccessful login attempts

Part 1 – Lock a user after a number of unsuccessful login attempts

Result:	Remark ID	Date	Signature
Passed		20-05-2014	HG / WK

Procedure

```
switch(config)# aaa new-model
switch(config)# aaa authentication login default local-case
switch(config)# aaa local authentication attempts max-fail 1
```

Part 2 - Unlock locked user

Result:	Remark ID	Date	Signature
Passed		20-05-2014	HG / WK

Procedure

```
switch# show aaa local user lockout
switch# clear aaa local user lockout username testusername
```

Part 3 - Create log event on login failure

Result:	Remark ID	Date	Signature
Passed		20-05-2014	HG / WK

Procedure

```
switch(config)# login on-failure log
```

2.3.4.2 4.2 System use notification

Part 1 - CLI

Result:	Remark ID	Date	Signature
Passed		20-05-2014	HG / WK

Procedure

```
switch(config)# banner login " Test banner "
```

Part 2 - GUI

Result:	Remark ID	Date	Signature
Failed		20-05-2014	HG / WK

Procedure

2.3.5 5 - Time

2.3.5.1 5.1 Change time

Part 1 - Change the time manually

Result:	Remark ID	Date	Signature
Passed		21-05-2014	HG / WK

Procedure

```
Switch# clock set 12:00:00 may 20 2014
```

Part 2 - Change the time using NTP

Result:	Remark ID	Date	Signature
Passed		21-05-2014	HG / WK

Procedure

```
switch(config)# ntp server 192.168.1.10
```

2.3.5.2 5.2 Authentication

Authenticate the NTP-server

Result:	Remark ID	Date	Signature
Passed		03-06-2014	HG / WK

Procedure

```
switch(config)# ntp authenticate
switch(config)# ntp authentication-key 1 md5 testntpkey
switch(config)# ntp server 192.168.1.10 key 1
```

2.3.6 6 - Port security general

2.3.6.1 6.1 Manual shutdown

Manually shut down a port

Result:	Remark ID	Date	Signature
Passed		21-05-2014	HG / WK

Procedure

```
switch(config)# interface fastethernet 1/5
switch(config-if)# shutdown
```

2.3.6.2 6.2 Rogue DHCP-server

Protect against rogue DHCP-servers

Result:	Remark ID	Date	Signature
Failed with remark	4	21-05-2014	HG / WK

Procedure

2.3.6.3 6.3 DHCP-rate-limit

Implement DHCP-rate-limit

Result:	Remark ID	Date	Signature
Failed with remark	5	21-05-2014	HG / WK

Procedure

2.3.7 7 - Port security against users

2.3.7.1 7.1 802.1x

Implement 802.1x user authentication

Result:	Remark ID	Date	Signature
Passed		21-05-2014	HG / WK

Procedure

```

switch(config)# aaa new-model
switch(config)# aaa group server radius RADIUS-GROUP
switch(config-sg-radius)# server-private 192.168.1.10 auth-port
1812 acct-port 1813 key password-radius
switch(config)# aaa authentication dot1x default RADIUS-GROUP
switch(config)# dot1x system-auth-control
switch(config)# interface fastethernet 1/3
switch(config-if)# switchport mode access
switch(config-if)# switchport access vlan 10
switch(config-if)# dot1x pae authenticator
switch(config-if)# authentication port-control auto

```

2.3.7.2 7.2 Port restrictions

Part 1 - Set a maximum number of users on a single port

Result:	Remark ID	Date	Signature
Passed		21-05-2014	HG / WK

Procedure

```

switch(config)# interface fastethernet 1/6
switch(config-if)# switchport port-security
switch(config-if)# switchport port-security maximum 2

```

Part 2 - Determine what MAC-addresses can communicate on a single port

Result:	Remark ID	Date	Signature
Passed		21-05-2014	HG / WK

Procedure

```

switch(config-if)# switchport port-security mac-address sticky
or
switch(config-if)# switchport port-security mac-address <mac-
address>

```

2.3.8 8 - Other functionality

2.3.8.1 8.1 Network segmentation

Logically segment the network using VLANs

Result:	Remark ID	Date	Signature
Passed		21-05-2014	HG / WK

Procedure

```
switch(config)# interface fastethernet 1/3
switch(config-if)# switchport mode access
switch(config-if)# switchport access vlan 10

switch(config)# interface fastethernet1/4
switch(config-if)# switchport mode access
switch(config-if)# switchport access vlan 20
```

2.3.8.2 8.2 Backup

Part 1 - Manually backup the configuration-file

Result:	Remark ID	Date	Signature
Passed		21-05-2014	HG / WK

Procedure

```
Switch# copy startup-config tftp:192.168.1.2/switch-config
```

Part 2 - Automated backup of configuration file.

Result:	Remark ID	Date	Signature
Passed		21-05-2014	HG / WK

Procedure

```
switch(config)# archive
switch(config-archive)# path tftp:192.168.1.2
switch(config-archive)# time-interval 1
```

2.3.8.3 8.3 Spanning-tree – block BPDUs

Block BPDUs on access-ports

Result:	Remark ID	Date	Signature
Passed		21-05-2014	HG / WK

Procedure

```
switch(config)# interface fastethernet 1/5
switch(config-if)# switchport mode access
```

```
switch(config-if)# spanning-tree portfast
switch(config-if)# spanning-tree bpduguard enable
```

2.3.8.4 8.4 Spanning-tree – protect the root switch

Protect the root switch in a spanning-tree topology

Result:	Remark ID	Date	Signature
Passed		21-05-2014	HG / WK

Procedure

```
switch(config)# interface fastethernet 1/1
switch(config-if)# switchport mode trunk
switch(config-if)# spanning-tree guard root
```

2.3.9 9 - Confidentiality

2.3.9.1 9.1 Encrypt passwords

Encrypt passwords in the configuration-file

Result:	Remark ID	Date	Signature
Passed		21-05-2014	HG / WK

Procedure

```
switch(config)# service password-encryption
```

2.3.9.2 9.2 Integrity check

Part 1 - Compute MD5/SHA1 checksum on configuration-file

Result:	Remark ID	Date	Signature
Passed		21-05-2014	HG / WK

Procedure

```
Switch# verify /md5 flash:cisco-ios.bin
```

Part 2 - Compute MD5/SHA1 checksum on firmware

Result:	Remark ID	Date	Signature
Passed		21-05-2014	HG / WK

Procedure

```
switch# verify /md5 nvram:startup-config
```

2.5 Conclusions of the test
Not applicable.